

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 09-252294

(43) Date of publication of application : 22. 09. 1997

(51) Int. Cl. H04L 9/08
G09C 1/00

(21) Application number : 08-202491 (71) Applicant : MITSUBISHI ELECTRIC CORP

(22) Date of filing : 31. 07. 1996 (72) Inventor : TAKEDA NORIKO
SHINODA SEIICHI
HASEYAMA HISAO

(30) Priority

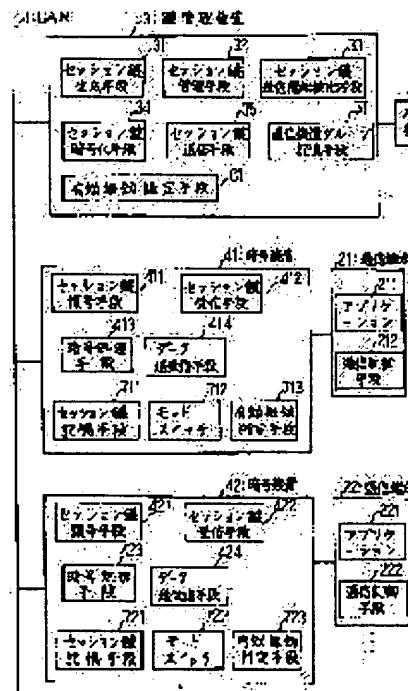
Priority number : 08 3997 Priority date : 12. 01. 1996 Priority country : JP

(54) CIPHERING SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain a ciphering system in which ciphered communication or plain text communication is selected by a ciphering device and a communication terminal equipment conducting ciphered communication and the ciphering device are easily grouped physically and logically.

SOLUTION: Ciphering device 41, 42 are provided with mode switches 712, 722 which store a session key to session key storage means 711, 721 and set whether or not communication data are ciphered/decoded by the session key. A key management device 3 delivers the individual session key for each group generated by a session key generating means 31 and valid/invalid information set by a valid/invalid setting means 61 as to whether the changeover of the mode switches 712, 722 of the ciphering devices is valid or invalid to each ciphering device. Valid/invalid discrimination means 713, 723 discriminate whether communication data are sent by ciphered communication or plain text communication based on the setting of the mode switches and the received valid/invalid information.



[Date of request for examination] 13.09.1996

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2812312

[Date of registration] 07.08.1998

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) ; 1998, 2000 Japanese Patent Office

特開平9-252294

(43)公開日 平成9年(1997)9月22日

(51) Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H04L 9/08			H04L 9/00	601 D
G09C 1/00	630	7259-5J	G09C 1/00	630 D
		7259-5J		630 E
			H04L 9/00	601 E

審査請求 有 請求項の数 20 O L (全 65 頁)

(21)出願番号	特願平8-202491
(22)出願日	平成8年(1996)7月31日
(31)優先権主張番号	特願平8-3997
(32)優先日	平8(1996)1月12日
(33)優先権主張国	日本 (JP)

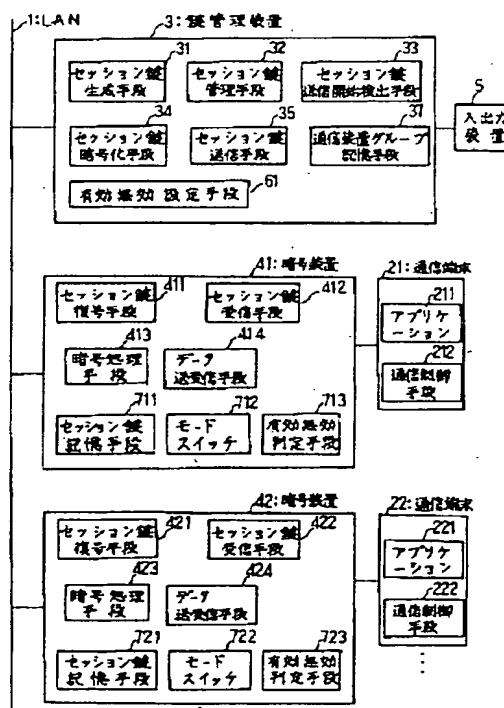
(71)出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(72)発明者	武田 紀子 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
(72)発明者	篠田 誠一 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
(72)発明者	長谷山 寿生 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
(74)代理人	弁理士 宮田 金雄 (外3名)

(54)【発明の名称】暗号化システム

(57)【要約】

【課題】 暗号通信を行う通信端末と暗号装置を、容易に物理的に又は論理的にグループ化できる暗号化システムを得る。また、暗号装置において暗号通信と平文通信の切り替えができる暗号化システムを得る。

【解決手段】 暗号装置41、42は、セッション鍵記憶手段711、721にセッション鍵を記憶し、セッション鍵により通信データを暗号化/復号するか否か設定するモードスイッチ712、722を備える。鍵管理装置3は、セッション鍵生成手段31が生成したグループ毎に個別のセッション鍵と、暗号装置のモードスイッチ712、722の切り替えを有効とするか無効とするか有効無効設定手段61が設定した有効無効情報を各暗号装置に配達する。暗号装置の有効無効判定手段713、723は、上記モードスイッチの設定と送信された上記有効無効情報とから、通信データを暗号通信とするか平文通信とするか判定する。



【特許請求の範囲】

【請求項 1】 グループ化された複数の通信装置と、少なくとも上記複数の通信装置の 1 つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも 1 つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えた暗号化システム。

【請求項 2】 上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも 1 つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする請求項 1 記載の暗号化システム。

【請求項 3】 上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、

上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする請求項 1 記載の暗号化システム。

【請求項 4】 上記暗号化条件は、通信相手となる 1 以上の通信装置により定まるることを特徴とする請求項 3 記載の暗号化システム。

【請求項 5】 上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まるることを特徴とする請求項 3 又は 4 いずれかに記載の暗号化システム。

【請求項 6】 上記暗号化条件は、通信方向により定まるることを特徴とする請求項 3 から 5 いずれかに記載の暗号化システム。

【請求項 7】 上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする請求項 3 から 6 いずれかに記載の暗号化システム。

【請求項 8】 上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする請求項 1 から 7 いずれかに記載の暗号化システム。

【請求項 9】 上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効

無効設定手段を備え、

上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする請求項 8 記載の暗号化システム。

【請求項 10】 上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする請求項 8 記載の暗号化システム。

10 【請求項 11】 上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、

上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする請求項 8 から 10 いずれかに記載の暗号化システム。

【請求項 12】 複数の鍵管理装置を備え、各鍵管理装置と 1 以上の暗号装置と 1 以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、

上記複数の鍵管理装置の中の 1 台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする暗号化システム。

【請求項 13】 上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも 1 つ記憶するセッション鍵記憶手段と、

上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、

上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、

通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、

上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、

上記鍵管理装置は、更に、

上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、

上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする請求項 1 2 記載の暗号化システム。

【請求項 14】 上記暗号化条件は、特定の通信に関する暗号化条件を設定した 1 以上の特例バスと上記特例バスに合致しない全ての通信に対する暗号化条件を設定した基本バスとからなることを特徴とする請求項 3 又は 13 記載の暗号化システム。

【請求項 15】 上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項 13 又は 14 いずれかに記載の暗号化システム。

【請求項 16】 上記暗号化条件は、通信方向により定まることを特徴とする請求項 13 から 15 いずれかに記載の暗号化システム。

【請求項 17】 上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする請求項 13 から 16 いずれかに記載の暗号化システム。

【請求項 18】 上記暗号化条件は、通信相手となる 1 以上の通信装置により定まることを特徴とする請求項 13 から 17 いずれかに記載の暗号化システム。

【請求項 19】 上記暗号装置は、通信装置あるいは鍵管理装置を接続する 1 以上のポートを備え、ポート毎に上記基本バスと上記特例バスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする請求項 14 から 18 いずれかに記載の暗号化システム。

【請求項 20】 上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする請求項 19 に記載の暗号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、通信網における暗号通信に関するものである。

【0002】

【従来の技術】 従来の暗号通信システムとして、例えば、社団法人電子情報通信学会発行の信学技報 O F S - 38 (1994-3) P7 ~ P12 「LAN 暗号通信方式の実装と評価」に示されるような通信端末及び鍵管理ワークステーション内に暗号通信ボードを置き、ローカルエリアネットワーク (以下 LAN とする) に接続する構成のシステムがある。図 19 は、このような従来の暗号通信システムを示す構成図である。図において、10 は LAN、210、220 はこの LAN 10 に暗号装置 410、420 を介して接続された通信端末、30 は鍵管理装置である。なお、図示していないが、通常は、更に多くの通信端末及び暗号装置が接続されている。

【0003】 通信端末 210、220 は、それぞれアプリケーション 2110、2210、通信制御手段 2120、2220、暗号通信制御手段 2130、2230 により構成される。鍵管理装置 30 は、セッション鍵生成手段 310、セッション鍵管理手段 320、セッション

鍵暗号化手段 340、セッション鍵送信手段 350、セッション鍵問い合わせ受信手段 360 により構成される。また暗号装置 410、420 は、それぞれセッション鍵復号手段 4110、4210、ユーザデータ暗号化／復号手段 4130、4230、ユーザデータ送受信手段 4140、4240、セッション鍵問い合わせ手段 4160、4260 により構成される。

【0004】 また、図 20 は、上記セッション鍵問い合わせ手段 4160 の詳細を示す構成図である。4161

10 はセッション鍵記憶手段、4162 はセッション鍵問い合わせ送信手段、4163 はセッション鍵受信手段である。なお、セッション鍵問い合わせ手段 4260 も同様の構成である。

【0005】 次に、このような従来の暗号通信システムにおけるデータ通信の手順につき説明する。暗号を用いて端末間で通信を行うには、通信する端末に接続されている暗号装置同士が共通のセッション鍵を持ち、そのセッション鍵によってデータの暗号化／復号を行う。通信する端末に接続されている暗号装置同士が共通のセッション鍵を持つための手順を鍵配達という。

【0006】 暗号通信を行う際には、鍵配達の手順と、実際のユーザデータの送受信の手順が必要である。従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたびに、これに先立って鍵配達の手順を行うものであった。

【0007】 ここでは、通信端末 210 のアプリケーション 2110 が、LAN 10 を介して接続されている通信端末 220 のアプリケーション 2210 と通信を行う際の鍵配達の手順につき説明する。以下の説明において、始めに通信を行おうとする通信端末 210 のアドレスを A とする。また、通信端末 220 のアドレスを B とする。

【0008】 図 21 は、従来の暗号通信システムにおけるセッション鍵の配達の手順を示すシーケンス図である。通信端末 210 のアプリケーション 2110 が、LAN 10 を介して接続されている通信端末 220 のアプリケーション 2210 と通信を行う際には、まずアプリケーション 2110 が通信制御手段 2120 を起動する。そして、通信相手の端末である通信端末 220 のアドレス B の情報を通信制御手段 2120 に渡す。通信制御手段 2120 は、通信端末 220 のアドレス B を記憶装置 (図示せず) に記憶するとともに、通信端末 220 のアドレス B の情報を暗号通信制御手段 2130 に渡す。

【0009】 暗号通信制御手段 2130 は、アドレス B の情報を含む通信開始要求コマンドを暗号装置 410 に送る。通信開始要求コマンドは、暗号装置 410 のセッション鍵問い合わせ手段 4160 のセッション鍵問い合わせ送信手段 4162 に渡される。セッション鍵問い合わせ合

わせ送信手段4162は、上記通信開始要求コマンドに含まれるアドレスBの情報を求め、アドレスBの情報を含む鍵配信要求コマンドKEYREQを生成し、これをLAN10を介して鍵管理装置30に送信する(S13)。また、セッション鍵記憶手段4161は、セッション鍵問い合わせ送信手段4162からのアドレスBの情報を記憶する。

【0010】次に、鍵管理装置30により受信された鍵配信要求コマンドKEYREQは、セッション鍵問い合わせ受信手段360に渡され、ここで鍵配信要求コマンドの発信元アドレスであるアドレスAを求め、これを鍵配信要求元アドレスとする。また、鍵配信要求コマンドKEYREQに含まれる情報よりアドレスBを求め、これを通信先アドレスとし、これらをセッション鍵管理手段320に渡す。セッション鍵管理手段320は、鍵配信要求元アドレスであるアドレスAと通信先アドレスであるアドレスBの組み合わせを、記憶装置(図示せず)に記憶するとともに、セッション鍵生成手段310を起動する。

【0011】セッション鍵生成手段310は、セッション鍵管理手段320により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段320に渡す。セッション鍵管理手段320は、このセッション鍵を記憶装置に記憶されている鍵配信要求元アドレスであるアドレスAと、通信先アドレスであるアドレスBの組み合わせとの組として記憶装置に記憶するとともに、セッション鍵暗号化手段340に渡す。

【0012】セッション鍵暗号化手段340は、このセッション鍵を予め設定されているセッション鍵を暗号化する鍵であるマスター鍵(鍵暗号化鍵)により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段320に渡す。セッション鍵管理手段320は、暗号化セッション鍵と、記憶装置に記憶されている鍵配信要求元アドレスであるアドレスAと、通信先アドレスであるアドレスBの組み合わせをセッション鍵送信手段350に渡す。セッション鍵送信手段350は、暗号化セッション鍵と、通信先アドレスであるアドレスBの情報を含んだセッション鍵配信コマンドKEYDISTを生成し、これを鍵配信要求元アドレスであるアドレスAの通信端末210に接続されている暗号装置410に対して送信する(S14)。

【0013】暗号装置410により受信されたセッション鍵配信コマンドKEYDISTは、セッション鍵問い合わせ手段4160のセッション鍵受信手段4163に渡される。セッション鍵受信手段4163は、セッション鍵配信コマンドKEYDISTより暗号化セッション鍵と通信先アドレスであるアドレスBの情報を求め、通信先アドレスであるアドレスBを記憶装置に記憶するとともに、暗号化セッション鍵をセッション鍵復号手段4110に渡す。

【0014】セッション鍵復号手段4110は、暗号化セッション鍵を予め設定されているマスター鍵により復号し、その結果をセッション鍵としてセッション鍵受信手段4163に渡す。セッション鍵受信手段4163は、セッション鍵をセッション鍵記憶手段4161に渡す。また、鍵管理装置30に対しセッション鍵受信確認コマンドKEYDIST_ACKを送信する(S15)。また、セッション鍵記憶手段4161は、記憶装置に記憶されている通信先アドレスであるアドレスBの情報と、該セッション鍵の組を記憶装置に記憶する。

【0015】鍵管理装置30により受信されたセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段350に渡され、該コマンドの発信元アドレスであるアドレスAを求め、これを鍵配信要求元アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段320に渡す。セッション鍵管理手段320は、該鍵配信要求元アドレスと記憶装置に記憶されている鍵配信要求元アドレスとを照合する。一致する鍵配信要求元アドレスとの組として記憶されている通信先アドレスであるアドレスBとセッション鍵の内、通信先アドレスであるアドレスBを記憶装置に記憶するとともに、セッション鍵暗号化手段340に該セッション鍵を渡す。

【0016】セッション鍵暗号化手段340は、該セッション鍵を予め設定されているマスター鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段320に渡す。セッション鍵管理手段320は、該暗号化セッション鍵と、記憶装置に記憶されている通信先アドレスであるアドレスBの組み合わせをセッション鍵送信手段350に渡す。セッション鍵送信手段350は、該暗号化セッション鍵と、記憶装置に記憶してある鍵配信要求元アドレスであるアドレスAの情報を含んだセッション鍵配信コマンドKEYDISTを生成する。これを通信先アドレスであるアドレスBの通信端末に接続されている暗号装置である暗号装置420に対して送信する(S16)。

【0017】暗号装置420では、上記暗号装置410と同様の動作が行われ、鍵管理装置30に対し、セッション鍵受信確認コマンドKEYDIST_ACKを送信する(S17)。鍵管理装置30により受信されたセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段350に渡され、該コマンドの発信元アドレスであるアドレスBを求め、これを通信先アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段320に渡す。

【0018】セッション鍵管理手段320は、該通信先アドレスと記憶装置に記憶されている通信先アドレスとを照合し、一致する通信先アドレスとの組として記憶されている鍵配信要求元アドレスであるアドレスAを、セッション鍵送信手段350に渡す。セッション鍵送信手段350は、該セッション鍵を記憶する。

段 350 は、記憶装置に記憶されている通信先アドレスであるアドレス B の情報を含んだ通信開始コマンド S T A R T を生成する。これを鍵配達要求元アドレスであるアドレス A の通信端末に接続されている暗号装置 410 に対して送信する (S 18)。

【0019】暗号装置 410 により受信された通信開始コマンド S T A R T は、ユーザデータ送受信手段 4140 に渡される。ユーザデータ送受信手段 4140 は、通信開始コマンド S T A R T より通信先アドレスであるアドレス B の情報を求め、これを記憶装置に記憶する。更に、通信端末 210 に鍵配達確認コマンドを送る。鍵配達確認コマンドは、通信端末 210 の暗号通信制御手段 2130 に渡される。暗号通信制御手段 2130 は、該鍵配達確認コマンドに含まれる通信先アドレスであるアドレス B の情報を求め、これを通信相手アドレスとし、該通信相手アドレスと通信開始フラグを ON とした情報との組を、記憶装置に記憶する。また、通信制御手段 2120 に該通信相手アドレスの情報を含む通信開始通知を渡す。以上の手順に従って、鍵配達が行われることにより、暗号装置 410 と暗号装置 420 が共通のセッション鍵を持つことができる。

【0020】次に、通信端末 210 のアプリケーション 2110 が、LAN 10 を介して接続されている通信端末 220 のアプリケーション 2210 と、通信を行う際のユーザデータの転送の手順につき詳細に説明する。通信端末 210 のアプリケーション 2110 は、ユーザデータと通信端末 220 のアドレス B との組を通信制御手段 2120 に渡す。通信制御手段 2120 は、該ユーザデータと通信端末 220 のアドレス B との組を暗号装置 410 に送る。

【0021】該ユーザデータと通信端末 220 のアドレス B との組は、ユーザデータ送受信手段 4140 に渡される。ユーザデータ送受信手段 4140 は、該ユーザデータと通信端末 220 のアドレス B との組をユーザデータ暗号化／復号手段 4130 に渡す。ユーザデータ暗号化／復号手段 4130 は、通信端末 220 のアドレス B により、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、通信相手アドレス B との組として記憶されているセッション鍵を用いて、該ユーザデータを暗号化する。これを暗号化ユーザデータとし、該暗号化ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段 4140 に渡す。ユーザデータ送受信手段 4140 は、該暗号化ユーザデータと通信相手アドレス B との組より、暗号化ユーザデータの情報を含むユーザデータ送信コマンドを暗号装置 420 に送る。

【0022】暗号装置 420 により受信されたユーザデータ送信コマンドは、ユーザデータ送受信手段 4240 に渡される。ユーザデータ送受信手段 4240 は、該ユーザデータ送信コマンドに含まれる暗号化ユーザデータ及び通信相手アドレス A の情報を求め、該暗号化ユーザ

データとアドレス A の組をユーザデータ暗号化／復号手段 4230 に渡す。ユーザデータ暗号化／復号手段 4230 は、通信相手アドレス A により、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、アドレス A との組として記憶されているセッション鍵を用いて、該ユーザデータを復号する。これをユーザデータとし、該ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段 4240 に渡す。ユーザデータ送受信手段 4240 は、該ユーザデータとアドレスとの組を通信端末 220 に渡す。通信端末 220 に渡された該ユーザデータと通信相手アドレスとの組は、通信制御手段 2220 に渡される。通信制御手段 2220 は、該ユーザデータと通信相手アドレスとの組をアプリケーション 2210 に渡す。

【0023】以上のように、従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたび毎に、これに先立って鍵配達の手順を行う必要がある。また、通信相手毎に暗号鍵の情報を登録する必要がある。また、暗号を用いるために、通信端末に暗号通信制御手段という特別の手段を追加する必要がある。

【0024】また、特開昭 54-93937 号には、複数ドメイン・データ通信ネットワークにおける“暗号装置用共通操作キー設定装置”について開示されている。

【0025】

【発明が解決しようとする課題】以上述べたように、従来の暗号データ通信の手順によれば、通信端末は各通信相手毎に通信を開始するに先立ち、その通信で用いるセッション鍵を鍵管理装置に要求し、それに応じて鍵管理装置から通信端末にセッション鍵を配達するようになっていた。そのため、同じ部所の通信端末同志をグループ化することに関しては、考慮されていなかった。また、暗号装置に接続された通信端末は、電子メール等の平文通信（暗号化されない通信）を送受信することができないという課題があった。また、通信相手となる通信端末、アプリケーション、通信方向により平文通信とするか暗号通信とするか、設定することはできなかった。また、複数の鍵の中から任意の鍵を用いて暗号化するという設定もできなかった。また、1 台の暗号装置に複数台の通信端末が接続される場合、通信端末毎に異なる条件で暗号化することはできなかった。また、特開昭 54-93937 号では、複数ドメイン間でデータ通信を暗号化するための共通の暗号化鍵を設定することが述べられていたが、共通の暗号化鍵を用い複数の重複したグループを実現する方式は、述べられていなかった。

【0026】本発明は、上記のような課題を解決するためになされたもので、1 つのネットワーク上の暗号データ通信を行う通信装置から、複数の物理グループを形成できる暗号化システムを提供することを目的とする。また、任意の暗号装置において、暗号通信と平文通信を切

り換えることができる暗号化システムを提供することを目的とする。また、同一のネットワーク上、あるいは、複数ドメイン間で複数の重複した論理グループを実現する暗号化システムを提供することを目的とする。

【 0 0 2 7 】

【課題を解決するための手段】この発明に係る暗号化システムは、グループ化された複数の通信装置と、少なくとも上記複数の通信装置の1つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えたことを特徴とする。

【 0 0 2 8 】上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも1つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする。

【 0 0 2 9 】上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする。

【 0 0 3 0 】上記暗号化条件は、通信相手となる1以上の通信装置により定まるることを特徴とする。

【 0 0 3 1 】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まるることを特徴とする。

【 0 0 3 2 】上記暗号化条件は、通信方向により定まるることを特徴とする。

【 0 0 3 3 】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする。

【 0 0 3 4 】上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする。

【 0 0 3 5 】上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報をから通

信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする。

【 0 0 3 6 】上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする。

【 0 0 3 7 】上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶された

10 グループに対応付けられた暗号装置に送信するセッション鍵送信手段と、上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする。

【 0 0 3 8 】この発明に係る暗号化システムは、複数の鍵管理装置を備え、各鍵管理装置と1以上の暗号装置と1以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、

20 それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、上記複数の鍵管理装置の中の1台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする。

【 0 0 3 9 】上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッ

30 ション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、上記鍵管理装置は、更に、上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする。

【 0 0 4 0 】上記暗号化条件は、特定の通信に関する暗号化条件を設定した1以上の特例バスと上記特例バスに合致しない全ての通信に対する暗号化条件を設定した基本バスとからなることを特徴とする。

【 0 0 4 1 】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まるることを特徴とする。

【 0 0 4 2 】上記暗号化条件は、通信方向により定まるることを特徴とする。

50 【 0 0 4 3 】上記暗号装置は、上記セッション鍵記憶手

段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする。

【0044】上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする。

【0045】上記暗号装置は、通信装置あるいは鍵管理装置を接続する1以上のポートを備え、ポート毎に上記基本バスと上記特例バスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする。

【0046】上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする。

【0047】

【発明の実施の形態】

実施の形態1. この実施の形態では、各暗号装置にセッション鍵を1つ記憶し、暗号通信と平文通信（暗号化しない通信）を切り換えることのできる暗号化システムについて述べる。

【0048】図1は、この実施の形態におけるネットワークシステムの一例を示す図である。2本のLAN (Local Area Network) がルータ/ブリッジ12によりLAN/WAN (Wide Area Network) 15と接続されているネットワークシステムである。LAN1には、鍵管理装置3が暗号装置49を介して接続される。更に、LAN1には、暗号装置41, 42, 43を介し、通信端末（通信装置とも言う）21, 22, 23が接続される。また、暗号装置を介さない通信端末24, 25が接続される。更に、ネットワーク管理装置13が接続される。図では、鍵管理装置3に暗号装置49が接続されているが、これは鍵管理装置3が他の通信端末と共にグループを構成する場合を想定している。そのため、鍵管理装置3に暗号装置49が接続されなくてもよい。また、1台の暗号装置に対し、複数台の通信端末を接続してもよい。

【0049】暗号装置41～43は、LAN1と通信端末21～23との間に置かれ、通信データのデータ部を暗号化/復号することで、LAN1上を流れる通信データの盗聴を防止する。ユーザデータの暗号化は、高速で秘匿性の高い独自の秘密鍵暗号方式による。暗号範囲は、暗号装置を出てネットワーク上を通り、通信先の暗号装置へ入るまでである。鍵管理装置3は、暗号装置に対するデータを暗号化するセッション鍵を配信するとともに、暗号装置41～43の状態を常時監視する。

【0050】図2は、この実施の形態における暗号化システムのブロック図である。図2において、LAN1に鍵管理装置3と暗号装置41, 42, ... が接続されている。鍵管理装置3には、入出力装置5が接続される。暗号装置41, 42, ... には、通信端末21, 22, ... が接続される。図には、暗号装置41, 42及び通信端末21, 22が図示されているが、通常は

更に多くの暗号装置及び通信端末が接続される。また、説明を簡単にするために、鍵管理装置3には、暗号装置が接続されない例を示してある。また、1台の暗号装置に対し、1台の通信端末が接続される例を図示してある。通信端末21, 22は、それぞれアプリケーション211, 221、通信制御手段212, 222から構成される。鍵管理装置3は、セッション鍵生成手段31、セッション鍵管理手段32、セッション鍵送信開始検出手段33、セッション鍵暗号化手段34、セッション鍵送信手段35、通信装置グループ記憶手段37、有効無効設定手段61からなる。セッション鍵生成手段31は、データを暗号化するセッション鍵を生成する。セッション鍵暗号化手段34は、セッション鍵生成手段31により生成されたセッション鍵を、鍵暗号化鍵を用いて更に暗号化する。セッション鍵送信手段35は、セッション鍵を各暗号装置に送信する。通信装置グループ記憶手段37は、グループ化された通信装置を記憶する。有効無効設定手段61は、暗号装置に備えられたモードスイッチの切り換えを有効とするか無効とするかを示す有効無効情報を、暗号装置毎に設定する。そして、設定した有効無効情報を対応する暗号装置に送信する。

【0051】暗号装置41, 42は、セッション鍵復号手段411, 421、セッション鍵受信手段412, 422、暗号処理手段413, 423、データ送受信手段414, 424、セッション鍵記憶手段711, 721、モードスイッチ712, 722、有効無効判定手段713, 723からなる。セッション鍵受信手段412, 422は、鍵管理装置3から送信された暗号化されたセッション鍵を受信する。セッション鍵復号手段411, 421は、セッション鍵受信手段412, 422により受信された暗号化されたセッション鍵を、それぞれの暗号装置独自の鍵暗号化鍵により復号する。暗号処理手段413, 423は、セッション鍵により通信データを暗号化、あるいは、復号する。データ送受信手段414, 424は、暗号処理手段413, 423により処理された通信データを送受信する。セッション鍵記憶手段711, 721は、通信データを暗号化、あるいは、復号するセッション鍵を少なくとも1つ記憶する。モードスイッチ712, 722は、この暗号装置における通信

データを、暗号通信とするか平文通信とするかを設定するスイッチである。有効無効判定手段713, 723は、暗号装置におけるモードスイッチ712, 722の設定と、鍵管理装置3から送信された有効無効情報から通信データを暗号通信とするか平文通信とするかを判定する。

【0052】セッション鍵と鍵暗号化鍵について述べる。セッション鍵は、ユーザデータを暗号化する鍵である。これに対し、鍵暗号化鍵は、セッション鍵を暗号化する鍵である。鍵暗号化鍵は、鍵管理装置3から各暗号装置にセッション鍵を配信する際、第三者にセッション

鍵を知られることなく配達するために用いる。鍵管理装置 3 のセッション鍵暗号化手段 3 4 で、セッション鍵を鍵暗号化鍵で暗号化する。暗号装置 4 1, 4 2 のセッション鍵復号手段 4 1 1, 4 2 1 で、配達された暗号化されたセッション鍵を、鍵暗号化鍵で復号する。鍵暗号化鍵は、暗号装置毎に異なる。鍵暗号化鍵の設定方法は、通信回線を介さない。

【0053】次に、鍵暗号化鍵の設定手順を述べる。

1. 鍵管理装置 3 で、各暗号装置毎に異なる鍵暗号化鍵を作成する。
2. 暗号装置に接続したローカルコンソールより鍵暗号化鍵を設定するコマンドを入力し、鍵入力モードにする。
3. 鍵管理装置で作成した鍵暗号化鍵を、暗号装置のローカルコンソールより入力する。
4. 暗号装置を立ち上げ直す。

【0054】セッション鍵は、ユーザデータを暗号化／復号するために使用する。同一グループの暗号装置のセッション鍵は、全て同じである。但し、後述の実施の形態述べるように、セッション鍵を複数用意すれば、暗号装置間で重複した論理グループを作ることが可能である。セッション鍵の設定方法は、オンラインで設定する。

【0055】次に、セッション鍵を暗号装置の要求に応じ、設定する手順の概略を述べる。

1. 鍵管理装置 3 で、セッション鍵を作成する。
2. 作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。
3. 暗号装置の電源を入れることにより、自動的に暗号装置からセッション鍵を送信してもらうよう要求コマンドが、鍵管理装置 3 へ送られる。
4. 鍵管理装置 3 から暗号化されたセッション鍵が要求のあった暗号装置へ送られる。

【0056】次に、他の方法として、セッションの鍵を管理者の指示により、設定する手順の概略を述べる。

1. 鍵管理装置 3 で、セッション鍵を作成する。
2. 作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号する。
3. 管理者の指示により、新しいセッション鍵を送信する暗号装置の範囲を決定する。範囲の種類は、大きく分けて、以下の 4 種類がある。
 - (1) 直前の暗号装置の状態確認の時に、電源が ON であった暗号装置全て。
 - (2) 直前の暗号装置の状態確認の時に、電源が ON で、かつ、予め指定されたグループ内の暗号装置全て。
 - (3) 指定された暗号装置。
 - (4) 全ての暗号装置。
4. 決定された範囲に含まれる暗号装置全てに、暗号化されたセッション鍵を配達する。

【0057】更に、他の方法として、鍵管理装置 3 にタ

イマを備え、一定時間が経過すると自動的にセッション鍵を生成し、同一グループに属する暗号装置に配達する手順を図 2 を用いて詳しく述べる。LAN 1 に接続され同一グループに属する各暗号装置に対し、一定時間毎にセッション鍵を鍵管理装置 3 から配布し、それまで設定されていたセッション鍵を直ちに配布されたセッション鍵で置き換える例である。通信端末 2 1 と通信端末 2

2. 即ち、暗号装置 4 1, 4 2 がグループ 1 としてグループ化され、通信装置グループ記憶手段 3 7 に登録されている。暗号通信を行う際には、鍵配達の手順と実際のユーザデータの送受信の手順が必要であるが、鍵配達の手順と実際のユーザデータの送受信の手順は、独立に行なうことが特徴である。

【0058】図 3 は、セッション鍵の配達の手順を示すシーケンス図である。S 1 はセッション鍵配達コマンド KEYDIST、S 2 はセッション鍵受信確認コマンド KEYDIST_ACK、S 3 はセッション鍵配達コマンド KEYDIST、S 4 はセッション鍵受信確認コマンド KEYDIST_ACK である。

- 20 20. 【0059】(手順 1-1) 鍵管理装置 3 のセッション鍵送信開始検出手段 3 3 のグループ 1 対応のタイマがタイムアウトすると、セッション鍵送信開始検出手信号をセッション鍵管理手段 3 2 に渡す。

(手順 1-2) セッション鍵管理手段 3 2 は、該セッション鍵送信開始検出手信号を受け取ると、セッション鍵生成手段 3 1 を起動する。

- 20 20. 【0060】(手順 1-3) セッション鍵生成手段 3 1 は、セッション鍵管理手段 3 2 により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段 3 2 に渡す。

(手順 1-4) セッション鍵管理手段 3 2 は、該セッション鍵をグループ 1 のセッション鍵として記憶装置に記憶する。セッション鍵管理手段 3 2 は、通信装置グループ記憶手段 3 7 からグループ 1 に属する暗号装置を検索し、暗号装置 4 1 を選ぶ。セッション鍵管理手段 3 2 は、セッション鍵暗号化手段 3 4 に該セッション鍵を渡し、暗号装置 4 1 に対する鍵暗号化である旨を知らせる。

- 40 40. (手順 1-5) セッション鍵暗号化手段 3 4 は、該セッション鍵を暗号装置 4 1 に対応する鍵暗号化鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段 3 2 に渡す。

【0061】(手順 1-6) セッション鍵管理手段 3 2 は、該暗号化セッション鍵と、暗号装置 4 1 のアドレスをセッション鍵送信手段 3 5 に渡す。

- 40 40. (手順 1-7) セッション鍵送信手段 3 5 は、該暗号化セッション鍵の情報を含んだセッション鍵配達コマンド KEYDIST を生成し、これを記憶装置に記憶する。セッション鍵送信手段 3 5 は、該セッション鍵配達コマンド KEYDIST を、渡されたアドレスにより暗号装

置 4 1 に対して送信する (S 1) 。

(手順 1-8) 暗号装置 4 1 のセッション鍵受信手段 4 1 2 により、該セッション鍵配達コマンド KEYD I S T は受信される。

(手順 1-9) セッション鍵受信手段 4 1 2 は、該セッション鍵配達コマンド KEYD I S T から暗号化セッション鍵を含むデータ部分を抽出し、セッション鍵復号手段 4 1 1 に渡す。

(手順 1-10) セッション鍵復号手段 4 1 1 は、該暗号化セッション鍵を含むデータ部分を、予め別の手段により設定されている暗号装置 4 1 独自の鍵暗号化鍵により復号する。そして、その結果をセッション鍵としてセッション鍵受信手段 4 1 2 に渡す。

【 0 0 6 2 】 (手順 1-11) セッション鍵受信手段 4 1 2 は、鍵管理装置 3 に対しセッション鍵受信確認コマンド KEYD I S T _ A C K を送信する (S 2) 。更に、該セッション鍵をセッション鍵記憶手段 7 1 1 に記憶する。

(手順 1-12) 鍵管理装置 3 により受信された暗号装置 4 1 からのセッション鍵受信確認コマンド KEYD I S T _ A C K は、セッション鍵送信手段 3 5 に渡される。セッション鍵送信手段 3 5 は、セッション鍵管理手段 3 2 に対し、暗号装置 4 1 へセッション鍵配達完了を通知する。セッション鍵管理手段 3 2 は、セッション鍵暗号化手段 3 4 にグループ 1 のセッション鍵を渡し、暗号装置 4 2 に対する暗号化である旨を知らせる。

(手順 1-13) セッション鍵暗号化手段 3 4 は、上記 (手順 1-5) と同様にして、暗号装置 4 2 に対応する暗号化セッション鍵を作成する。セッション鍵送信手段 3 5 は、該暗号化セッション鍵の情報を含んだセッション鍵配達コマンド KEYD I S T を作成し、暗号装置 4 2 に送信する (S 3) 。

(手順 1-14) 暗号装置 4 2 のセッション鍵受信手段 4 2 2 により、該セッション鍵配達コマンドは受信される。

(手順 1-15) セッション鍵受信手段 4 2 2 は、該セッション鍵配達コマンドから暗号化セッション鍵を抽出し、該暗号化セッション鍵をセッション鍵復号手段 4 2 1 に渡す。

【 0 0 6 3 】 (手順 1-16) セッション鍵復号手段 4 2 1 は、該暗号化セッション鍵を予め別の手段により設定されている独自の鍵暗号化鍵により復号する。その結果をセッション鍵として、セッション鍵受信手段 4 2 2 に渡す。

(手順 1-17) セッション鍵受信手段 4 2 2 は、鍵管理装置 3 に対しセッション鍵受信確認コマンド KEYD I S T _ A C K を送信する (S 4) 。更に、該セッション鍵をセッション鍵記憶手段 7 2 1 に記憶する。

(手順 1-18) 鍵管理装置 3 により、受信されたセッション鍵受信確認コマンド KEYD I S T _ A C K は、

セッション鍵送信手段 3 5 に渡される。

(手順 1-19) セッション鍵送信手段 3 5 は、暗号装置 4 2 へのセッション鍵配達完了をセッション鍵管理手段 3 2 に通知する。セッション鍵管理手段 3 2 は、グループ 1 に属する他の暗号装置がないことから、グループ 1 に対する鍵配達は、完了したと判断する。

【 0 0 6 4 】 以上的手順に従って、鍵配達が行われることにより、同一グループに属する暗号装置 4 1 と暗号装置 4 2 が共通のセッション鍵を持つことができる。この

10 後、通信端末 2 1 のアプリケーション 2 1 1 が、 L A N 1 を介して接続されている通信端末 2 2 のアプリケーション 2 2 1 と通信を行う。アプリケーション 2 1 1 のユーザデータは、暗号装置 4 1 の暗号処理手段 4 1 3 で暗号化され、暗号装置 4 2 の暗号処理手段 4 2 3 で復号され、アプリケーション 2 2 1 に渡される。

【 0 0 6 5 】 また、上記のセッション鍵送信開始検出手段 3 3 におけるセッション鍵送信開始検出信号をタイムによらず、鍵管理装置 3 の管理者による手動の入力操作により、出力するようにしてもよい。また、上記のセッション鍵送信開始検出手段 3 3 におけるセッション鍵送信開始検出信号を、暗号装置の立ち上げ状態を検出することにより出力するようにしてもよい。

【 0 0 6 6 】 なお、上記 2 台の暗号装置へ鍵配達を行う手順を示したが、同一のグループに属する任意の台数の暗号装置に対しても、同様に行うことができる。セッション鍵の変更を、セッション鍵の配達／受信と同時にを行う例を示した。しかし、通信を一度停止してからセッション鍵を新しい鍵に変更してもよいし、セッション鍵の配達／受信から所定時間経過後に変更してもよい。

30 【 0 0 6 7 】 次に、本実施の形態の要点である暗号通信と平文通信の切り換えについて述べる。図 4 は、暗号化システムにおけるグループ分けを説明するための図である。鍵管理装置 3 は、暗号装置 4 9 を介し、 L A N 1 に接続される。通信端末 2 0 ～ 2 2 、 2 5 ～ 2 9 は、暗号装置 4 1 ～ 4 6 を介し、 L A N 1 に接続される。通信端末 2 1 と 2 2 は、同一の暗号装置 4 2 に接続される。通信端末 2 8 と 2 9 は、同一の暗号装置 4 6 に接続される。更に、通信装置 2 3 、 2 4 が暗号装置を介さず、 L A N 1 に接続されている。鍵管理装置 3 と暗号装置 4 9 40 は、グループ A とする。暗号装置 4 1 ～ 4 3 と通信端末 2 0 ～ 2 2 、 2 5 は、グループ B とする。暗号装置 4 4 ～ 4 6 と通信端末 2 6 ～ 2 9 は、グループ C とする。ここで、例えば、通信端末 2 0 から送信されたユーザデータは、暗号装置 4 1 で暗号化される。暗号化されたデータを受信できる可能性のある通信端末は、通信端末 2 1 、 2 2 、 2 5 である。暗号装置を介さない通信端末 2 3 、 2 4 とグループ C に属する通信端末 2 6 ～ 2 9 は、通信データを復号できないため、受信することができない。このように、暗号通信において、同一暗号グループ 50 の暗号装置に接続されている通信端末間は、あたかも平

文通信のように通信できる。しかし、暗号グループが異なる又は暗号装置が接続されていない通信端末では、暗号化された通信文を受信しても復号できないため盗聴できない。もし、暗号装置そのものを盗まれても、どの暗号グループに属しているかは、暗号装置側からは見分けられないので、なりすましも防げる。

【0068】ところが、暗号グループが異なる又は暗号装置が接続されていない通信端末と通信したい場合は、暗号装置から出入りする通信を、暗号化／復号することを止めなければならない。この切り換えを暗号装置41, 42, ... が持っているモードスイッチ712, 722, ... のON／OFFで実現する。モードスイッチ712, 722, ... をONすると、平文通信となり、OFFにすると、暗号通信となる。しかし、暗号装置は、通信端末利用者が勝手に操作できるため、モードスイッチのON／OFFのみで暗号通信を平文通信に変更できるのは、セキュリティ上好ましくない。そこで、鍵管理装置でモードスイッチの切り換えを有効とするか無効とするか、暗号装置毎に有効無効情報を設定する。これにより、鍵管理装置で平文通信と暗号通信の切り換えができる暗号装置を管理することができる。

【0069】図5は、鍵管理装置3で設定された有効無効情報と有効無効情報を入力する画面である。新たにデータを入力する場合は、入力フィールドから入力する。入力フィールドから入力するデータとして、グループナンバ(GN)、IPアドレス、備考、有効／無効情報がある。画面に表示されるグループ名称は、グループナンバ(GN)が入力されると自動的に画面に出力される。有効無効情報は、予め‘0’(無効)がセットされている。有効としたい場合は、‘1’を入力する。表示されているデータは、上から順に図4で示した暗号装置49, 41～46に対応する。暗号装置41と46の有効無効情報が有効とされている。ここで、有効とは、該暗号装置のモードスイッチの切り換えが有効という意味である。無効とは、暗号装置でモードスイッチが切り換えられても、無効とするという意味である。

【0070】鍵管理装置3が暗号化されたセッション鍵を、各暗号装置へKEYDISTコマンドにより配信する際、有効無効情報も付加して送る。図6において、プロトコルタイプは、通信プロトコルのタイプを示す。認証用データは、配信された暗号装置で復号できたか否かチェックするための固定パターンである。暗号装置で復号されたデータの一部が固定パターンと一致すれば、復号が正しく行われたことを示す。最後のビットに、有効無効情報がセットされる。‘1’は有効を示し、‘0’は無効を示す。以上のように、KEYDISTコマンドの内容の内、データが設定されない部分は、0とする。そして、セッション鍵及び有効無効情報などが設定されたKEYDISTコマンドの内容は、鍵暗号化鍵で暗号化さ

れ送信される。

【0071】鍵管理装置3における有効無効設定手段61は、入力画面により設定された有効無効情報を、セッション鍵配信コマンドKEYDISTを生成するセッション鍵送信手段35に渡す。セッション鍵送信手段35は、図6で示したように、最後のビットに有効無効情報をセットしたKEYDISTコマンドを生成する。次に、暗号装置41を例に取ると、セッション鍵受信手段412がKEYDISTコマンドを受信し、セッション鍵復号手段411に渡す。セッション鍵復号手段411が復号し、復号したセッション鍵をセッション鍵受信手段412に渡す。セッション鍵受信手段412は、復号されたKEYDISTの内容から有効無効情報を取り出し、有効無効判定手段713に渡す。有効無効判定手段713は、モードスイッチ712のスイッチのON／OFFと、有効無効情報の論理積によって暗号通信とするか平文通信とするか判定する。

【0072】図7に、モードスイッチの情報と有効無効情報の論理積を表として示す。モードスイッチOFFは(0)であり、ONは(1)である。有効無効情報が、有効は(1)であり、無効は(0)である。そのため、論理積を取ると、モードスイッチONであり、かつ、有効無効情報が有効の場合のみ(1)、即ち、ユーザデータは透過となる。それ以外の場合は、全てモードスイッチの設定如何に関わらず、暗号化される。なお、透過とは、平文通信とすることである。

【0073】図8は、図4のように、グループ化された暗号化システムにおいて、平文通信を採用する場合である。暗号装置41, 43, 44, 46のモードスイッチがONとなっている。即ち、これらの暗号装置は、平文通信とするモードスイッチが切り換えられている。ところが鍵管理装置3の有効無効情報は、図5で示したように、暗号装置41と46のみ有効となっている。そのため、通信端末20から送られたユーザデータは、暗号装置41では暗号化されず、平文で送信される。平文通信であるため、暗号装置のない通信端末23, 24で受け取ることができる。また、暗号装置46のモードスイッチがONであり、有効無効情報が有効であるため、通信端末20からの通信データを復号しない。そのため、通信端末28, 29は、通信端末20の送出した平文通信を受け取ることができる。暗号装置43, 44は、モードスイッチがONではあるが、有効無効情報が無効となっているため、平文通信を受け取ることができない。また、暗号装置41は、グループBに属するが、暗号装置46は、グループCに属する。平文通信とすることにより、暗号装置のない通信端末、あるいは、異なるグループの通信端末とでも通信することができる。

【0074】以上のように、この実施の形態の暗号化システムは、暗号装置のセッション鍵をグループ単位で同じものとすることにより、異なるグループ間の通信を禁

止することができる。また、ネットワーク上の盗聴を防止することができる。更に、暗号通信とするか平文通信とするか、暗号装置側及び鍵管理装置の設定で選択することができ、異なるグループの通信端末、あるいは、暗号装置を持たない通信端末と通信することもでき、より柔軟な暗号化システムを形成することができる。更に、暗号装置のモードスイッチにより、暗号通信とするか平文通信とするか設定し、加えて鍵管理装置で暗号装置のモードスイッチが有効であるか無効であるか一括管理することができるため、より確実なセキュリティ管理が行える。

【0075】また、図2の暗号装置のブロック図において、暗号装置41、42のモードスイッチ712、722を取り去ってもよい。この場合、鍵管理装置3の有効無効設定手段61で、有効と設定した暗号装置を平文通信とすると決めてもよい。有効無効設定手段61で無効と設定した暗号装置は、暗号通信を行う。有効無効設定手段61で設定した有効無効情報は、鍵管理装置3から暗号装置41、42の有効無効判定手段713、723に送信され、各暗号装置の有効無効判定手段が暗号通信とするか平文通信とするか判定する。

【0076】また、図2の暗号化システムのブロック図において、鍵管理装置3の有効無効設定手段61と、暗号装置41、42の有効無効判定手段713、723を省いてもよい。この場合、暗号装置41、42のモードスイッチ712、722のON/OFFにより、暗号通信とするか平文通信とするか設定する。

【0077】また、図9に、鍵管理装置3aがセッション鍵を配達しない場合のブロック図を示す。図9に示すように、鍵管理装置3aは、図2で示したセッション鍵送信開始検出手段33、セッション鍵暗号化手段34、セッション鍵送信手段35を省く。暗号装置41a、42aは、セッション鍵復号手段411、421、セッション鍵受信手段412、422を省く。この場合、鍵管理装置3aにおいて、通信装置グループ記憶手段37に記憶されたグループ毎に、セッション鍵をセッション鍵生成手段31により生成する。鍵管理装置3aで生成されたセッション鍵は、ネットワークを用いた通信によらず、各暗号装置のセッション鍵記憶手段に記憶する。他の働きは、上述の説明と同様である。

【0078】図10に、図2で示した暗号化システムの鍵管理装置がない場合を示す。LAN1に暗号装置41b、42bを介し、通信端末21、22が接続される。暗号装置及び通信端末は、図示していないが、他にも接続されている。暗号装置41b、42bは、セッション鍵記憶手段711、721、暗号処理手段413、423、データ送受信手段414、424、モードスイッチ712、722からなる。通信端末21、22は、図2と同様である。セッション鍵は、セッション鍵生成手段と同様の働きを有する処理装置において作成され、それ

ぞれ暗号装置41b、42bのセッション鍵記憶手段711、721に入力され、記憶される。セッション鍵の同じ暗号装置同志が同一グループとなる。モードスイッチ712、722のスイッチのON/OFFにより、暗号通信とするか平文通信とするか決まる。

【0079】実施の形態2. この実施の形態は、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか、暗号化条件を設定することができる暗号化システムについて述べる。更に、複数のセッション鍵を1台の暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか、暗号化条件を設定することができる暗号化システムについて述べる。

【0080】図11は、この実施の形態における暗号化システムのブロック図である。LAN1に鍵管理装置6と暗号装置81、82が接続されている。鍵管理装置6には、入出力装置5が接続されている。暗号装置81、82には、通信端末21、22が接続されている。鍵管理装置6は、セッション鍵生成手段31、セッション鍵管理手段32、セッション鍵送信開始検出手段33、セッション鍵暗号化手段34、セッション鍵送信手段35、通信装置グループ記憶手段37、暗号化条件設定手段62からなる。暗号装置81は、セッション鍵復号手段411、セッション鍵受信手段412、暗号処理手段413、データ送受信手段414、セッション鍵記憶手段711、暗号化条件記憶手段811、条件判定手段812からなる。暗号装置82も同様の構成である。通信端末21、22は、図2と同様である。暗号装置の暗号化条件記憶手段811、821は、通信データの暗号化に関する暗号化条件を記憶する。暗号化条件としては、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか設定する。更に、複数のセッション鍵を暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか暗号化条件で設定する。暗号化条件記憶手段811、821は、これらの暗号化条件を記憶する。

暗号化条件を設定するのは、鍵管理装置6の暗号化条件設定手段62により鍵管理装置6の管理者が、それぞれの暗号装置に条件を設定し、各暗号装置に送信する。あるいは、鍵管理装置6の暗号化条件設定手段62は省き、それぞれの暗号装置における暗号化条件記憶手段811、821において、それぞれの暗号装置の使用者が暗号化条件を、暗号化条件記憶手段811、821に設定してもよい。条件判定手段812、822は、暗号化条件記憶手段811、821に記憶された暗号化条件と受信した通信データの通信相手となる通信装置、通信方向、アプリケーション、更に複数のセッション鍵がある場合には、セッション鍵により平文通信とするか暗号通信とするか、あるいは、いずれのセッション鍵を用いるか判定する。

【 0 0 8 1 】 図 1 2 は、この実施の形態における暗号化システムを利用したネットワークシステムの例である。サーバ 9 1、WWW (W o r l d W i d e W e b) 代理サーバ 9 2、メールサーバ 9 4 がルータ 1 4 を介してインターネット 1 6 につながっている。また、WWW 9 3 がインターネット 1 6 に接続されている。暗号装置 8 1、8 2 が、LAN 1 に接続されている。暗号装置 8 1 は、通信端末 2 1、2 2 を接続する。暗号装置 8 2 は、通信端末 2 3、2 4 を接続する。LAN 1 には、この他にも暗号装置及び通信端末が接続されているが、図では省く。暗号装置 8 1、8 2 は、グループ A に属する。

【 0 0 8 2 】 図 1 2 のネットワーク例において、暗号装置 8 1 の暗号化条件を次のように設定する。

基本バス：アプリケーション（全）、暗号

特例 1：IP アドレス（メールサーバ）& アプリケーション（メール）& 通信方向（出）、透過

特例 2：IP アドレス（WWW 代理サーバ）& アプリケーション（h t t p）& 通信方向（出）、透過

特例 3：IP アドレス（サーバ）& アプリケーション（ネームサーバ）、透過

【 0 0 8 3 】 上記の暗号化条件は、基本バスと特例バスがあるが、特例バスで示した条件の方が優先順位は高い。通常の通信は、基本バスで指定された暗号化条件に従う。しかし、特例 1、2、3 で指定された暗号化条件に適合する通信データの場合、特例バスで示された条件

を優先する。図 1 2 を用いて説明すると、通信端末 2 1、あるいは、2 2 からグループ A 内の通信端末 2 3、あるいは、2 4 へ通信を送る場合は、基本バスの暗号化条件に従い、全てのアプリケーションの通信データについて暗号化する。この通信の流れを図では、点線で示す。通信端末 2 1、2 2 からメールサーバ 9 4 へメールを送る場合、特例 1 の暗号化条件に適合し透過、即ち、平文通信となる。通信端末 2 1、2 2 から WWW 代理サーバ 9 2 にアプリケーション（h t t p）のユーザデータを送信する場合、特例 2 に適合し平文通信となる。通信端末 2 1、2 2 からサーバ 9 1 へアプリケーション（ネームサーバ）で通信データを送受信する場合、特例 3 に従い平文通信となる。特例 3 では、通信方向を指定していないので、送受信する両方向のデータについて透過、即ち、平文通信となる。なお、暗号装置 8 2 の暗号化条件は、暗号装置 8 1 と異なってもよい。また、暗号装置に複数の通信端末が接続されている場合は、接続された端末毎に異なる暗号化条件（特例バス）を設定してもよい。なお、基本バス、特例バスについては、後述の実施の形態で更に詳しく説明する。このように、1 台の暗号装置でグループ内の通信は暗号化し、公共的なメールサービスや WWW サービスを平文で受けることができる。

【 0 0 8 4 】 図 1 3 は、この実施の形態における暗号化

システムの他のネットワーク例である。インターネット 1 6 に、WWW サーバ 9 5 とメールサーバ A 9 6 が接続されている。ルータ 1 4 を介し、2 本の LAN 1 が接続され、一方の LAN 1 に暗号装置 8 1 が接続される。暗号装置 8 1 には、通信端末 2 1 と社内メールサーバ 9 7 が接続される。また、もう一方の LAN 1 には暗号装置 8 2 が接続される。暗号装置 8 2 には、社内メールサーバ 9 8 と通信端末 2 2 が接続される。暗号装置 8 1 と 8 2 及び通信端末 2 1、2 2、社内メールサーバ 9 7、9 8 は、同一のグループに属する。

【 0 0 8 5 】 図 1 3 のネットワーク例において、暗号装置 8 1 の暗号化条件を次のように設定する。

基本バス：アプリケーション（メール+WWW）、透過
特例 1：IP アドレス（全ての社内の暗号装置のアドレス）& アプリケーション（全）、暗号

【 0 0 8 6 】 上記のように、暗号化条件を設定すると、暗号装置 8 1 を通過する全ての社内メールや社内のアプリケーション・データは暗号化され、インターネット 1 6 に接続された公共のメールサーバ A 9 6 のメールや、

WWW サーバ 9 5 との通信データのやりとりは透過、即ち、平文通信となる。このように、インターネットに接続された通信装置であっても暗号装置を介すことにより、同一社内で 1 つのグループを形成し、通信データのやりとりは暗号化することができる。そのため、インターネットを介した通信であっても、監聽を防ぐことができる。

【 0 0 8 7 】 図 1 4 は、暗号化システムを用いた他のネットワーク例である。LAN/WAN 1 5 に、LAN 1 がルータ 1 4 を介し 3 本接続されている。LAN 1 に

30 は、暗号装置 8 1 ～ 8 5 が接続されている。通信端末 2 1 ～ 2 9 は、暗号装置に接続されている。通信端末 2 0 は、暗号装置を介さず、LAN 1 に接続されている。人事ファイルサーバ 9 9 は、暗号装置 8 3 に接続されている。

【 0 0 8 8 】 図 1 4 のネットワーク例において、暗号装置 8 4 の暗号化条件を次のように設定する。

基本バス：アプリケーション（全）、セッション鍵 A により暗号

特例 1：IP アドレス（人事ファイルサーバ）& アプリケーション（全）、セッション鍵 B により暗号

【 0 0 8 9 】 図 1 4 において、グループ A は、セッション鍵 A によるグループである。例えば、技術部のグループとする。グループ B は、セッション鍵 B によるグループである。例えば、これを人事部とする。グループ B には、人事ファイルサーバ 9 9 があり、一般的のアクセスは禁止したい。上記のように、暗号化条件を設定すると、通信端末 2 7 からセッション鍵 A を用いると、グループ A 内の全ての通信端末と全てのアプリケーションについて通信データを送受信できる。通信端末 2 7 からは、セッション鍵 B を用いて人事部、即ち、グループ B の人事

ファイルサーバ 26 と全てのアプリケーションに関し、通信データを送受信できる。そのため、通信端末 27 のユーザを人事権のある役員とする。このように、暗号装置に複数のセッション鍵を保有し、暗号化条件でどのセッション鍵を使用するか設定することにより、いろいろなグループの組み合わせを重複して作ることができる。そのため、セッション鍵による暗号化条件の設定により監聽防止及びアクセス制御ができ、人事課や役員しかアクセスできない人事情報サーバなどを社内 LAN に接続できる。

【0090】図 15 は、暗号化システムを用いた他のネットワーク例である。WAN 17 は、ルータ 14 を介し、2 本の LAN 1 と接続されている。それぞれのルータ 14 の LAN 1 側に、暗号装置 81 と 82 を接続する。これにより、例えば、社内全体を 1 つのグループ、グループ A とすることができます。2 本の LAN 1 には、暗号装置 83 と 84 がそれぞれ接続されている。暗号装置 83 と 84 には、通信端末 23, 24, 27, 28 が接続されている。しかし、更に、多くの通信端末を暗号装置にそれぞれ接続してもよい。また、LAN 1 には、暗号装置を介さずに通信端末 21, 22, 25, 26 が接続されている。しかし、更に、多くの通信端末を接続してもよい。暗号装置 83 と 84 及び暗号装置に接続された通信端末でグループ B が形成される。グループ B を例えば、人事部とする。グループ B は、グループ A に属する。しかし、暗号装置 83, 84 を介さないグループ A の通信端末 21, 22, 25, 26 からは、グループ B の通信端末 23, 24, 27, 28 と通信データのやりとりをすることはできない。また、通信端末 21, 22, 25, 26 は、相互に通信データを送受信できるが、通信データは暗号化されない。暗号化されるのは、例えば、通信装置 21 が通信装置 25 に通信データを送受信したい場合、通信装置 21 側の LAN 1 に接続された暗号装置 81 で暗号化され、WAN 17 を介し暗号装置 82 で復号されるまでである。暗号装置 82 で復号された通信データは、平文通信で通信端末 25 に届く。即ち、WAN 17 のような公衆網を通る時に、暗号化され監聽を防止することができる。このように、暗号装置を配置することにより監聽を防止できるため、従来専用線でしか構築できなかったシステムが公衆網を利用することができます。

【0091】図 16 は、アプリケーションとセッション鍵により暗号化条件を定めることにより、重複した複数のグループ化ができるることを説明する図である。暗号装置 81 ~ 83 が、LAN 1 に接続されている。暗号装置 81 では、アプリケーション 1 ~ 4 と 6 を実行する。暗号装置 82 では、アプリケーション 1, 3, 5, 6 を実行する。暗号装置 83 では、アプリケーション 1, 2, 4 ~ 6 を指定する。同一番号のアプリケーションが登録されている暗号装置間では、同じセッション鍵で通信デ

ータを暗号化／復号するとする。これにより、アプリケーション 1, 6 が指定されている暗号装置 81 ~ 83 で、グループ A が形成される。アプリケーション 2, 4 が指定されている暗号装置 81, 83 で、グループ B が形成される。アプリケーション 3 が指定されている暗号装置 81, 82 で、グループ C が形成される。アプリケーション 5 が指定されている暗号装置 82 と 83 で、グループ D が形成される。このように、暗号化条件の指定の仕方により、上記のように、3 台の暗号装置を様々に組み合わせ、重複した複数のグループを形成することができる。なお、この例では、アプリケーションを例としたが、通信プロトコルのタイプによりグループ化してもよい。暗号装置に 1 つのセッション鍵しか保有できない場合、暗号装置とセッション鍵が 1 対 1 で対応するので、セッション鍵をどの暗号装置に持たせるかにより、暗号装置のグループ化をする。この場合、物理的ネットワークのグループを形成することができる。暗号装置に複数のセッション鍵を保有できる場合は、アプリケーションや通信プロトコルなどの機能とセッション鍵の組み合わせにより、1 台の暗号装置が重複して複数のグループに属することができる。これは、物理的ネットワークグループに対し、論理的ネットワークグループということができる。

【0092】図 17 は、図 11 で鍵管理装置 6a がセッション鍵は生成するが、暗号装置 81a, 82a にネットワークを介して配送しない場合のブロック図を示す。暗号化条件の設定及び暗号化条件の判定は、上述した通りである。

【0093】図 18 は、図 11 において、鍵管理装置を省く場合のブロック図である。各暗号装置で保有するセッション鍵は、鍵管理装置 6 のセッション鍵生成手段 31 と同等の機能を有する処理装置で作成し、暗号装置 81b のセッション鍵記憶手段 711 に入力し記憶される。この場合も複数のセッション鍵を作成し、セッション鍵記憶手段 711 に記憶することは可能である。暗号装置 81b, 82b は、セッション鍵記憶手段 711, 721、暗号処理手段 413, 423、データ送受信手段 414, 424、暗号化条件記憶手段 811, 821、条件判定手段 812, 822 からなる。暗号化条件は、それぞれ暗号装置のユーザが暗号化条件記憶手段 811, 821 に記憶する。暗号化条件による論理的ネットワークグループの形成は、上記説明と同様である。なお、上記実施の形態で述べたモードスイッチを暗号装置に備えてもよい。この場合、暗号化条件がどのようなものであっても、モードスイッチが ON であれば、平文通信に切り換わるとする。

【0094】以上のように、この暗号化システムを用いることにより、専用線でしか構築できなかった監聽防止システムが、公衆網やインターネットを利用して構築することができる。また、ネットワークを使った情報サー

ビスにおいて、暗号鍵を持つユーザのみがアクセスすることができるグループ化を図ることができる。また、人事課や役員しかアクセスできない人事情報サーバなどを社内LANに接続できる。この場合、暗号化条件の設定により一般のユーザが人事情報サーバを監視することができないし、アクセスすることもできない。また、暗号化条件の機能（通信プロトコル、アプリケーション）とセッション鍵の指定の仕方により、複数の重複した論理グループを同一のネットワーク上に構築することができる。

【0095】実施の形態3. この実施の形態は、1台の暗号装置に複数の通信端末が接続される場合、通信端末を接続するポート毎に暗号化のための条件を基本バスと特例バスにより設定することができる暗号化システムについて述べる。

【0096】図19は、この実施の形態で用いるネットワークシステムを示す図である。図において、暗号装置81～84は、通信端末が1台接続されるNODE型暗号装置である。暗号装置51、52は、通信端末が複数台接続されるHUB型暗号装置である。暗号装置81、暗号装置51、暗号装置82は、これらの暗号装置に接続される通信端末20～23、25とともに、グループAを形成する。暗号装置83、84と暗号装置52は、それぞれに接続される通信端末26～29とともに、グループBを構成する。鍵管理装置7はLAN1に接続され、暗号装置81～84と暗号装置51、52の暗号化／復号に用いるセッション鍵を生成し、各暗号装置に配布する。また、通信端末24は、平文通信のみ行える端末である。

【0097】図20に、1台の暗号装置に1台の通信端末が接続されるNODE型暗号装置81を示す。暗号装置81には、平文ポートと暗号ポートがあり、平文ポートには、通信端末20が1台接続される。通信端末20と暗号装置81の間をながれるデータは、暗号化されない平文である。暗号装置81の暗号ポートは、LAN1に接続される。暗号ポートを流れるデータは、暗号化されたデータである場合もあるし、平文の場合もある。NODE型暗号装置は、接続の制限として平文ポート側に1台の通信端末のみが接続され、別のHUBやブリッジ／ルータの接続は、禁止である。また、暗号化条件で指定する通信方向は、平文ポートから暗号ポートにデータが流れる方向を（出）、即ち、出方向と定義する。図21に、1台の暗号装置に複数台の通信端末が接続されるHUB型暗号装置51を示す。暗号装置51の平文ポートには、通信端末21、22、23が接続される。暗号装置51の暗号ポートは、LAN1に接続される。HUB型暗号装置の接続の制限としては、平文ポート側には複数のポートを備え、1つのポートに1台の端末のみが接続され、別のHUBやブリッジ／ルータの接続は、禁止である。暗号化条件で用いる通信方向（出）は、図に

示すように、平文ポートから暗号ポートへ流れる方向とする。

【0098】図22は、この実施の形態で用いる鍵管理装置7と暗号装置81、暗号装置51、通信端末20～23のブロック図である。鍵管理装置7は、上記実施の形態で述べた図11における鍵管理装置6に、ポート条件設定手段63が加わったものである。暗号装置51は、通信端末21～23が接続されるHUB型暗号装置である。暗号装置51は図11における暗号装置82の

10 暗号化条件記憶手段821が、ポート条件記憶手段921に置き換わったものである。ポート条件記憶手段921は、通信端末を接続するポート毎に、上記実施の形態で述べた基本バスと特例バスをポート条件として記憶する。条件判定手段822は、ポート条件記憶手段921に設定されているポート条件と通信端末21～23より入力された通信データの条件（通信データを用いるアプリケーション、通信方向、通信相手となる通信装置）とを比較し、ポート条件記憶手段921に記憶された基本バスと特例バスの中の何れのバスを用いるか判定し、基本バス、あるいは、特例バス設定されたセッション鍵で暗号化するか、あるいは、平文通信とするか決定する。暗号装置81は、通信端末20を1台接続するNODE型暗号装置である。入出力装置5と暗号装置81と通信端末20～23は、図11と同様である。

【0099】鍵管理装置7におけるポート条件設定手段63は、鍵管理者がHUB型暗号装置のポート条件を設定し、対象となるHUB型暗号装置51、・・・におけるポート条件記憶手段921・・・に配布する。しかし、暗号装置51、・・・において、それぞれポート条件を設定し、ポート条件記憶手段921・・・に設定するならば、鍵管理装置7におけるポート条件設定手段63は省いてもよい。しかし、鍵管理装置7のポート条件設定手段63で、暗号装置のポート条件を設定することにより一括管理が可能となる。セッション鍵記憶手段711、721は、鍵管理装置7のセッション鍵生成手段31で生成された鍵と、暗号化条件記憶手段811またはポート条件記憶手段921に設立される鍵の識別名称との対応を記憶する。例えば、暗号化条件記憶手段811に記憶される基本バスと特例バスで鍵A、鍵B、鍵Cと記述するとする。セッション鍵記憶手段711、721には、セッション鍵の識別名称、鍵A、鍵B、鍵Cとそれぞれに対応する鍵管理装置7から配信されたセッション鍵を記憶する。このようにすることにより、暗号化条件とポート条件を設定する鍵管理者が実際のセッション鍵を知る必要がない。また、セッション鍵の秘密性を守るために、定期的にセッション鍵を鍵管理装置7で生成し変更する場合、暗号化条件とポート条件にセッション鍵の識別子で指定するため、暗号化条件とポート条件をセッション鍵の更新の度に変更する必要がない。

【0100】図23に、暗号化条件記憶手段811に記

憶する暗号化条件の例を示す。図 23 の暗号化条件を以下に記す。

基本バス：アプリケーション（全），鍵A

特例バス0：宛先IPアドレス（全）&アプリケーション（メール），透過

特例バス1：宛先IPアドレス（通信端末26）&アプリケーション（AP11）&通信方向（出），鍵B

このように、暗号化条件としては、基本バスと特例バスを記憶することができる。基本バスは、デフォルトとして扱われるバスで、特例バスに合致しない通信は全て基本バスで扱われる。そのため、宛先IPアドレスの指定はできない。一方、特例バスは、宛先IPアドレスを必ず設定し、特例バスで設定された条件に合致する通信は、該当特例バスで設定されたセッション鍵により暗号化される。あるいは、透過設定された場合は、暗号化せず、平文のまま暗号装置から出力される。基本バスと特例バスでは、特例バスは指定しなくてもよい。即ち、暗号化条件は、少なくとも基本バスを設定しなければならない。なお、基本バスと特例バスに合致しない通信は、全て廃棄される。

【0101】次に、基本バスと特例バスの特徴をそれぞれ述べる。基本バスは、NODE型暗号装置では、平文ポートが1つなので1つ設定可能である。基本バスでは、宛先IPアドレスは指定できないが、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。アプリケーションフィルタは、特定のアプリケーション名の指定が可能であり、その他全通過、あるいは、全廃棄の指定が可能である。また、データが暗号装置の平文ポートから暗号ポートへ、出力するか入力するかによる通信方向フィルタの設定ができる。通信方向は、図20、図21に示したように、平文ポートから暗号ポートへデータが流れる方向を出方向（出）とする。反対に、暗号ポートから平文ポートへデータが流れる場合、入方向（入）とする。更に、出方向及び入方向を合わせた両方向の指定が可能である。両方向を指定する場合は、基本バス及び特例バスに通信方向を明記しなければ、両方向扱いとなる。セッション鍵は、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する場合に用いる。セッション鍵は、基本バスの場合、暗号装置の属するグループの鍵に固定する。また、セッション鍵を指定せず、透過設定（平文通信）とすることも可能である。

【0102】特例バスは、複数種類設定することができる。この実施の形態では、1台の暗号装置で最大64設定することができる。特例バスでは、宛先IPアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。特例バスでは、宛先IPアドレスを指定しなければならない。また、IPアドレスの有効ビット長も併せて指定する。

暗号化条件の通信相手は、条件設定としてIPアドレス

とIPアドレスの有効ビット長という2項目を設定する。IPアドレスは、4つの数字をドット（.）で区切って表現する。各数値は、0～255までの範囲を取ることが可能である。0～255の数値は、2進数で表現すると8ビットで表すことができるので、有効ビット長により（8ビット×4）桁の内、どこまでのビットをそのまま使用するのかを指定する。有効ビット長で範囲外とされたビットは0であると見なす。例えば、133.141.70.151というIPアドレスで、有効ビット長=32ビットの場合は、通信相手となる通信装置は1つだけで、133.141.70.151のIPアドレスを持つ通信装置となる。しかし、同じ133.141.70.151というIPアドレスで、有効ビット長=24ビットとすると、133.141.70.0～133.141.70.255までの256通りのIPアドレスのうちいずれかのIPアドレスを持つ複数の通信装置が通信相手となる。このように、IPアドレスの有効ビット長指定により通信相手となる通信装置は1つであったり、複数であったりする。特例バスのアプリケーションフィルタ、通信方向フィルタに関しては基本バスと同じ仕様である。セッション鍵は、宛先IPアドレスフィルタ、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する。セッション鍵は、セッション鍵記憶手段711に複数のセッション鍵を記憶することにより、複数のセッション鍵の中から1つを選んで特例バスに指定することができる。セッション鍵は、特例バス毎に1個指定する。または、平文通信とする透過設定にすることも可能である。また、特例バスでは、宛先IPアドレスを指定するという特性から、

例えは、IPブロードキャストアドレスは、扱うことができない。即ち、ブロードキャストを使用するようなアプリケーションは、特例バスでは扱えず、基本バスの中で扱うことになる。

【0103】図24に、ポート条件記憶手段921に記憶するポート条件の例を示す。図24におけるポート条件を以下に記す。

ポート1

基本バス1：アプリケーション（全），鍵A

ポート2

40 基本バス2：アプリケーション（メール），透過

特例バス1：宛先IPアドレス（通信端末26）&アプリケーション（AP11）&通信方向（出），鍵B

ポート3

基本バス3：アプリケーション（AP22）&通信方向（入），鍵A

特例バス1：宛先IPアドレス（通信端末26）&アプリケーション（AP11）&通信方向（出），鍵B

特例バス2：宛先IPアドレス（通信端末28）&アプリケーション（SPPR），鍵C

50 【0104】HUB型である暗号装置51は、複数のボ

ートを備え、図22の例では、3台の通信端末21～23が接続されている。そのため、ポート1、ポート2、ポート3毎に、それぞれポート条件を記憶する。ポート条件としては、基本バスと特例バスを指定することができる。基本バスと特例バスの特徴は、上述した通りであるが、NODE型暗号装置とHUB型暗号装置では次のような相違がある。NODE型暗号装置における基本バスは、装置当たり1つ指定する。HUB型暗号装置では、ポート毎に1つの基本バスを設定する。特例バスは、HUB型暗号装置では、複数ポートで共有可能である。基本バスと特例バスでは、特例バスは指定しなくともよい。即ち、ポート条件は、各ポート毎に少なくとも基本バスを設定しなければならない。

【0105】特例バスと基本バスの優先順位は、特例バスが優先される。また、特例バスが複数ある場合は、特例バスそれぞれに予め優先順位を与えておくこともできる。この実施の形態では、暗号条件記憶手段、ポート条件記憶手段に記憶する特例バスの順番で優先順位を与える。

【0106】図25に、図24に示したポート条件を例にポート条件における基本バスと特例バスの関係を述べる。図25に示す模式図では、ポート1は、基本バスだけである。ポート2は、基本バスと特例バス1、ポート3は、基本バスと2つの特例バス1、2を持つ。また、特例バス1は、ポート2とポート3で共有しているところを示している。更に、パイプの途中に挿入されている楕円形のふるいに当たる部分が、各種の選択処理を表している。図の楕円形に()内に記したものは、図24のポート条件である。例えば、特例バス2を例にとると、宛先IPアドレスフィルタにおける(28)は、通信端末28を示す。アプリケーションフィルタ(SPPR)は、アプリケーションSPPRを表す。通信方向フィルタにおける(両)は、通信方向が両方向であることを示す。セッション鍵(C)は、セッション鍵の識別子として鍵Cを示す。また、基本バス1、3で指定するセッション鍵は、暗号装置が属するグループのセッション鍵Aであり、固定である。基本バス2には透過を設定する。

【0107】基本バスと特例バスをこのように設定することができるため、暗号化することによるセキュリティ強化とともに、ユーザの利便性を考慮していくつかの選択性を提供することができる。例えば、通常暗号ワールドにいるユーザがネットニュースを平文で運用したいという要望に答え、ニュースサーバとの通信だけ例外的に平文で行うことが可能となる。また、特例バスを用い、グループに与えられたセッション鍵以外のセッション鍵を指定することができるため、予め設定されたグループを物理グループとすると、この物理グループに属しながら新たな論理グループを形成することができる。新たな論理グループを形成する条件は、宛先IPアドレス、ア

プリケーション、通信方向、セッション鍵であり、これらの組み合わせにより設定することができる。

【0108】図26に、図19に示したネットワークシステムにおいて、暗号装置81、51で図23、図24に示す暗号化条件とポート条件を設定することにより形成される新たな論理グループを示す。グループAに属する通信端末20、22、23は、特定のアプリケーション(AP11)の場合、通信端末26に通信データを出力することができる。通信端末20、22、23は、グループAに属するが、特例バス1を設定することによりグループBの通信端末26と新たな論理グループ1を形成する。論理グループ1は、アプリケーション(AP11)を通信端末20、22、23で処理しているときに形成されるグループである。また、更に、通信方向が通信端末20、22、23から通信端末26に出力される場合に限り形成されるグループである。論理グループ2は、図24のポート3における特例バス2で設定された条件により生ずるグループである。この場合、論理グループ2は、通信端末23において、アプリケーション

20 (SPPR)が実行される際、通信端末28とデータのやりとりをする場合に生じるグループである。このように、特例バスの設定により予め定められたグループを越えて新たな論理グループを形成することが可能となる。また、特例バスの設定の仕方により、例えば、グループAの中に1以上のサブグループを形成することも可能となる。また、1台の暗号装置に複数台の通信端末が接続されていても、ポート毎にポート条件を設定することにより各通信端末毎に異なった使い方が可能となる。例えば、図24の例であると、通信端末21は、グループAにのみ属する。通信端末22は、基本的には、アプリケーション(メール)のための通信端末とし、他のアプリケーション(メール)を行う通信端末と、グループ分けに関わらずデータ交換が平文で可能となる。また、アプリケーション(AP11)を実行する際、通信端末22から通信端末26にデータを送信する端末となる。通信端末23は、アプリケーション(AP22)を行う場合、他の通信端末から通信を受信する端末として基本的に動作する。また、アプリケーション(AP11)を実行し、通信端末26にデータを送信する端末となる。また、アプリケーション(SPPR)を実行することができる、通信端末28と通信のやりとりを行なうことができる端末である。このように、1つの暗号装置に接続されていながら、各通信端末毎にそれぞれ性格の異なる役割を分担することができる。

【0109】図27は、HUB型暗号装置を用いた通信形態の例を示す。暗号装置51のとともに、通信端末21、22が接続され、暗号装置52のとともに、通信端末23とDBサーバ904が接続され、セッション鍵1によるグループ1が形成される。暗号装置53のとともに、通信端末24、25が接続され、暗号装置54のとも

に、通信端末 26 と DB サーバ 905 が接続され、セッション鍵 2 によりグループ 2 を形成する。暗号装置 51 ～ 54 は、HUB 型暗号装置である。暗号装置 51 のポート 2 に接続された通信端末 22 が EO A サーバ 901、ニュースサーバ 902、WWW サーバ 903 とは、平文通信を行い、かつ、DB サーバ 905 とも通信を行う。この場合暗号装置 51 に、図 28 に示すポート条件（ポート 2 のみを記す）を設定する。

基本バス：アプリケーション（全）、鍵 1

特例 1：宛先 IP アドレス（aaa）&アプリケーション（AP23）&通信方向（出）、透過

特例 2：宛先 IP アドレス（bbb）&アプリケーション（A119）&通信方向（出）、透過

特例 3：宛先 IP アドレス（ccc）&アプリケーション（T80）&通信方向（出）、透過

特例 4：宛先 IP アドレス（ddd）&アプリケーション（AP1523）&通信方向（出）、鍵 2

【0110】ここで、aaa は EO A サーバの IP アドレスであり、bbb はニュースサーバの IP アドレスであり、ccc は WWW サーバの IP アドレスであり、ddd は DB サーバ 905 の IP アドレスである。基本バスは、グループ 1 に属することを定義し、全てのアプリケーションについて、かつ、両方向通信について、セッション鍵 1 で暗号化／復号を行うことを意味する。特例バス 1 は、EO A サーバと平文通信を行うための設定である。特例バス 2 は、ニュースサーバと平文通信を行うための設定である。特例バス 3 は、WWW サーバと平文通信を行うための設定である。特例バス 4 は、DB サーバ 905 とセッション鍵 2 により暗号通信を行うための設定である。

【0111】図 29 に、LAN に接続する暗号装置を示す。LAN に接続する暗号装置 501 は、平文ポートから入力された暗号化されていないデータを暗号化し、暗号ポートから出力する。平文ポート側の接続に制限はない。図 30 と図 31 に、LAN に接続する暗号装置 501 の設置例を示す。図 30 では、ルータ 142 と広域網に接続されたルータ 141 側に暗号装置 501 の暗号ポートを接続する。暗号装置 501 の平文ポートには、ルータ 143 とブリッジ 151 が接続される。ルータ 143 とブリッジ 151 から入力される暗号化されていないデータが、暗号装置 501 の平文ポートに入力され、暗号装置 501 で暗号化されて暗号ポートから出力される。暗号化されたデータは、ルータ 141 を介し広域網を通り、通信相手先へ通信される。または、暗号化されたデータは、ルータ 142 を介し通信相手先へ通信される。図 31 は、LAN に接続する暗号装置 501、502 の第 2 の設置例である。広域網にルータ 141 が接続され、ルータ 141 にイーサネット・スイッチ 131、132 が接続される。イーサネット・スイッチ 131 の 1 つのポートに、LAN に接続する暗号装置 501 の暗

号ポートが接続される。暗号装置 501 の平文ポートが、一般 HUB 121 に接続される。暗号装置 502 に關しても同様である。一般 HUB 121、あるいは、122 から入力される暗号化されていないデータが暗号装置 501、あるいは、502 の平文ポートに入力され、暗号化されて暗号ポートからイーサネット・スイッチ 131、あるいは、132 に出力される。暗号装置 501、502 の暗号ポート側、即ち、イーサネット・スイッチ 131、132 とルータ 141 を介した広域網側では、暗号化されたデータとなる。

【0112】図 32 は、LAN に接続する暗号装置を用いた通信形態を示す図である。子会社 A と子会社 B と本社は、インターネット 16 を介し通信を行う。子会社 A は、暗号装置 501 をインターネット 16 側のルータ 143 に接続する。子会社 B は、暗号装置 502 をインターネット 16 側のルータ 144 に接続する。本社は、暗号装置 503 をインターネット 16 側のルータ 145 に接続する。これにより、本社、子会社 A、子会社 B との間で通信を行う場合、暗号装置 501、502、503 によりインターネット側では通信データが暗号化されるため、通信のセキュリティが保たれる。本社と子会社 A とは、セッション鍵 5 を用いた通信を行う。本社は、子会社 B とはセッション鍵 6 を用いて WWW サーバアクセスだけを行う。また、本社からインターネット 16 上の各種公開サーバ 906 とは、平文でアクセスを行いたい。このような通信形態を行う際の本社にある暗号装置 503 での暗号化条件を、図 33 に示す。

基本バス 1：アプリケーション（全）、透過

特例 1：IP アドレス（aaa）&アプリケーション（全）、鍵 5

特例 2：IP アドレス（bbb）&アプリケーション（AP80）&通信方向（出）、鍵 6

ここで、aaa は子会社 A に設置されたルータ 141 の IP アドレスである。bbb は子会社 B に設置されたルータ 142 の IP アドレスである。なお、LAN に接続する暗号装置には、平文ポートが 1 本なのでポート条件ではなく、暗号化条件を記憶する。

【0113】以上のように、この実施の形態では、1 台の暗号装置が複数のポートを備え、それぞれのポートに

40 通信端末が複数接続される場合、ポート毎に暗号化に関するポート条件を記憶することができる暗号化システムについて述べた。これにより、暗号通信、平文通信を設定できるとともに、宛先 IP アドレス、アプリケーション、通信方向、セッション鍵によりポート毎に暗号化する条件を設定することができる。そのため、予め設定された通信装置からなる物理グループの暗号化通信以外に、柔軟に宛先 IP アドレス、アプリケーション、通信方向、セッション鍵により新たな論理グループを設定することができる。また、同じ暗号装置に接続される通信端末であっても、それぞれのポート条件を変えることが

できるため、通信端末を1台毎に異なった使い方ができ、ユーザにとって使いやすい暗号化システムを提供することができる。

【0114】実施の形態4. この実施の形態は、鍵管理装置と暗号装置と通信端末により暗号管理ドメインを形成し、複数の暗号管理ドメイン間で共通セッション鍵を持つことにより、異なる暗号管理ドメイン間の暗号化通信が可能な暗号化システムについて述べる。また、暗号化条件とポート条件に共通セッション鍵を設定することにより、異なる暗号管理ドメインに属する通信端末からなる論理グループを形成する暗号化システムについて述べる。

【0115】図34は、この実施の形態における暗号化システムのネットワークシステムを示す図である。暗号管理ドメインA, B, Cに分けられ、それぞれ1台の鍵管理装置と複数台の暗号装置と複数台の通信端末とからなる。暗号管理ドメイン間は、ルータ14とLAN/WAN15によりネットワーク接続されている。暗号管理ドメインA～Cは、通常それぞれに属する鍵管理装置71～73がセッション鍵を生成し、管理するため、暗号管理ドメイン相互間の暗号化通信はできない。そこで、共通セッション鍵を複数の暗号管理ドメインで共有することにより、暗号管理ドメイン間の暗号化通信を行う。この実施の形態では、複数ある鍵管理装置の内、1台の鍵管理装置をマスタ鍵管理装置とし、共通セッション鍵を生成し、他の鍵管理装置に配送する。ここでは暗号管理ドメインAの鍵管理装置71をマスタ鍵管理装置とし、共通セッション鍵を生成し配送するものとする。鍵管理装置72及び鍵管理装置73を鍵管理装置71から共通セッション鍵を受け取る鍵管理装置とする。なお、共通セッション鍵に対し、暗号管理ドメイン内で用いるセッション鍵をローカル鍵と呼ぶことにする。

【0116】図35に、鍵管理装置71, 72のブロック図を示す。鍵管理装置71, 72には、図22に示した鍵管理装置7にセッション鍵テーブル64が加わる。鍵管理装置71, 72におけるセッション鍵生成手段31が複数のセッション鍵を生成し、セッション鍵テーブル64に記憶する。この実施の形態では、鍵管理装置71～73でそれぞれ最大32個のセッション鍵を生成するものとする。図36に、セッション鍵テーブル64の例を示す。セッション鍵テーブル64は、鍵番号と、鍵作成可否を示す許可フラグと、生成された鍵と、その鍵に対する属性を記憶する欄がある。鍵番号1から鍵番号32に対応して、共通セッション鍵とローカル鍵を鍵の欄に記憶する。セキュリティ強化のため一定時間毎にローカル鍵は生成され、更新される。共通セッション鍵は更新不可のため、許可フラグを「非作成」(図ではXで示す)とする。共通セッション鍵に対し暗号管理ドメインA, B間の共通セッション鍵であることを記憶するために属性欄に"共通(A, B)"と書き込まれている。

鍵管理装置72は、図22の鍵管理装置7にセッション鍵テーブル64に加え、更に、セッション鍵受信手段65とセッション鍵復号手段66が加わったものである。セッション鍵受信手段65とセッション鍵復号手段66は、鍵管理装置71から暗号化されて配送される共通セッション鍵を受信し、復号する。なお、鍵管理装置71～73の通信装置グループ記憶手段37は、暗号管理ドメインA～C毎に鍵管理装置と暗号装置と通信端末のアドレスを記憶する。他の構成要素は、上記実施の形態で述べた構成要素と同様であるので、説明は省略する。また、NODE型暗号装置81～88とHUB型暗号装置51～54は、図22で述べたブロック図と同様であるので、説明は省略する。

【0117】暗号管理ドメインAでは、鍵管理装置71が共通セッション鍵とローカル鍵を複数生成し、暗号管理ドメインAに属する暗号装置81～83と暗号装置51に配送する。また、共通セッション鍵は鍵管理装置71, 72に配送する。更にセキュリティ強化のため、鍵管理装置71はローカル鍵を定期的に生成し、各暗号装置のローカル鍵を更新する。また、鍵管理装置71は、暗号化条件設定手段62により暗号装置81～83の暗号化条件記憶手段811～831に暗号化条件を設定する。鍵管理装置71のポート条件設定手段63は、暗号装置51のポート条件記憶手段921にポート条件を設定する。また、暗号管理ドメインB, Cにおいても、鍵管理装置72, 73が同様に暗号管理ドメイン内で用いるローカル鍵を定期的に生成する。また、共通セッション鍵は鍵管理装置71から配送されたものを使う。鍵管理装置72, 73がローカル鍵と共通セッション鍵を用いて暗号化条件及びポート条件を所属する暗号装置に設定する。

【0118】次に、鍵管理装置71が共通セッション鍵を生成し配送する手順を述べる。初めに、暗号管理ドメインAと暗号管理ドメインBとの間で鍵番号5, 8, 32を共通セッション鍵とすると、取り決めてある場合について述べる。

(1) 鍵管理装置71のセッション鍵生成手段31が32個のセッション鍵を生成する。
 (2) セッション鍵生成手段31でセッション鍵が32個生成されると、セッション鍵管理手段32は、セッション鍵テーブル64に作成したセッション鍵を書き込む。セッション鍵管理手段32は、セッション鍵テーブル64の鍵番号5, 8, 32に対応する許可フラグを「非作成」とする(図では、X印)。更に、鍵番号5, 8, 32に対応する属性欄に、暗号管理ドメインAと暗号管理ドメインB間の共通セッション鍵であることを示す"共通(A, B)"を書き込む。
 (3) セッション鍵管理手段32は、暗号管理ドメインBに生成した共通鍵1～3を配送するため、セッション鍵暗号化手段34で共通鍵1～3を暗号化し、セッション

ン鍵送信手段 3 5 で、暗号管理ドメイン B の鍵管理装置 7 2 へ送信する。

【0 1 1 9】 (4) 暗号管理ドメイン B の鍵管理装置 7 2 におけるセッション鍵受信手段 6 5 は、鍵管理装置 7 1 のセッション鍵送信手段 3 5 から送信された、暗号化された共通セッション鍵を受信する。鍵管理装置 7 2 におけるセッション鍵管理手段 3 2 は受信された、暗号化された共通セッション鍵をセッション鍵復号手段 6 6 に渡す。セッション鍵復号手段 6 6 は、暗号化された共通セッション鍵を復号する。鍵管理装置 7 2 におけるセッション鍵管理手段 3 2 は、復号された共通セッション鍵をセッション鍵テーブル 6 4 の鍵番号 5, 8, 3 2 に対応する鍵の欄に書き込み、許可フラグを「非作成」とする。また、セッション鍵テーブル 6 4 の鍵番号 5, 8, 3 2 に対応する属性欄に、暗号管理ドメイン A と暗号管理ドメイン B 間の共通セッション鍵であることを示す“共通 (A, B)”を書き込む。鍵管理装置 7 2 のセッション鍵テーブル 6 4 において、鍵番号 5, 8, 3 2 に既に共通セッション鍵が書かれている場合は、上書きされる。

(5) 鍵管理装置 7 2 のセッション鍵生成手段 3 1 は、自暗号管理ドメインのためのローカル鍵を生成する。セッション鍵管理手段 3 2 は、セッション鍵テーブル 6 4 の許可フラグが「作成」(図では、○印)となっている鍵番号に、セッション鍵生成手段 3 1 が生成したセッション鍵をローカル鍵として書き込む。鍵管理装置 7 1, 7 2 のローカル鍵は、上記実施の形態で述べたと同様な方法で自暗号管理ドメインの暗号装置に配送される。

【0 1 2 0】 次に、鍵管理装置 7 1 が共通セッション鍵を生成し配送する他の手順について述べる。暗号管理ドメイン A, B, C で暗号通信するための共通セッション鍵を共通鍵 1 とする。暗号管理ドメイン A, B が暗号通信するための共通セッション鍵を共通鍵 2 とする。暗号管理ドメイン A, C が暗号通信するための共通セッション鍵を共通鍵 3 とする。暗号管理ドメイン B, C が暗号通信するための共通セッション鍵を共通鍵 4 とする。この場合、鍵管理装置 7 1 が共通鍵 1 ~ 4 を生成し、暗号管理ドメイン B の鍵管理装置 7 2 に共通鍵 1, 2, 4 を配送する。暗号管理ドメイン C の鍵管理装置 7 3 には、共通鍵 1, 3, 4 を配送する。初めに述べた方法では、鍵管理装置 7 1 と 7 2 の間で鍵番号 5, 8, 3 2 を共通セッション鍵を登録する鍵番号と決めていた。しかし、例えば、鍵管理装置 7 1 が生成した 3 2 個のセッション鍵の中から任意に 4 個の共通鍵 1 ~ 4 を選び出し、該当する許可フラグを「非作成」とする。鍵管理装置 7 1 は、セッション鍵テーブル 6 4 の属性欄にどの暗号管理ドメイン間の共通セッション鍵とするかを書き込む。更に鍵管理装置 7 1 は、該当する鍵管理装置に共通セッション鍵と属性情報を配送する。配送された鍵管理装置では、セッション鍵テーブル 6 4 における共通セッション

鍵を記憶していた任意の鍵番号の位置に共通セッション鍵を書き込み、許可フラグを「非作成」とし、属性にどの暗号管理ドメインとの共通セッション鍵かを書き込む。このような方法で、各暗号管理ドメインに共通セッション鍵を配送管理してもよい。

【0 1 2 1】 暗号管理ドメイン B, C で、それぞれ必要とする共通鍵 1 ~ 4 を配送された後、各鍵管理装置 7 1 ~ 7 3 は、上記実施の形態 3 で述べたように、自暗号管理ドメイン内の暗号装置に対し、暗号化条件設定手段 6 10 2 とポート条件設定手段 6 3 を用いて暗号化条件とポート条件を設定する。暗号化条件とポート条件における基本バスと特例バスの設定については、上記実施の形態と同様であるので説明は省略する。図 3 7 に、共通鍵 1 ~ 4 を用いて暗号化条件とポート条件を設定した場合形成される暗号管理ドメインを越えた論理グループの例を示す。通信端末 2 c, 2 d, 2 h, 2 k が、共通鍵 1 により暗号化／復号される暗号通信を行う論理グループ 1 を形成する。通信端末 2 a, 2 b, 2 f が、共通鍵 2 により暗号化／復号される暗号通信を行う論理グループ 2 を形成する。通信端末 2 d, 2 l, 2 m が、共通鍵 3 により暗号化／復号される暗号通信を行う論理グループ 3 を形成する。通信端末 2 e, 2 f, 2 j, 2 k は、共通鍵 4 により暗号化／復号される暗号通信を行う論理グループ 4 を形成する。このように、それぞれ独自のセッション鍵を有する暗号管理ドメイン間で共通セッション鍵を共有することにより、暗号管理ドメインの壁を越えた新たな論理グループが通信端末間で形成される。

【0 1 2 2】 以上のように、この実施の形態では、鍵管理装置と暗号装置と通信端末とからなる暗号管理ドメインが複数あり、各暗号管理ドメインは、鍵管理装置が暗号管理ドメイン内のローカル鍵を生成し管理する。これらの暗号管理ドメイン間で暗号通信を行うための共通セッション鍵を共有し、かつ、暗号条件とポート条件を共通セッション鍵を用いて設定することにより、異なる暗号管理ドメインに属する通信端末同士が共通セッション鍵で暗号化された暗号通信を行うことができる。また、基本バス及び特例バスの設定において、宛先 IP アドレス、アプリケーション、通信方向、セッション鍵を設定することが可能であるため、異なる暗号管理ドメイン間の通信端末間で論理グループを形成することができる。また、宛先 IP アドレス、アプリケーション、通信方向で共通セッション鍵による暗号通信を設定することができるため、ユーザサイドの利便性とともに、セキュリティの向上を図ることができる。

【0 1 2 3】

【発明の効果】 以上のように、この発明によれば、グループ化された複数の通信装置間で通信データを暗号化、あるいは、復号することができる。

【0 1 2 4】 また、この発明によれば、モードスイッチの設定により、暗号通信と平文通信とのいずれかを選択

することができる。

【0125】また、この発明によれば、暗号装置毎に通信データの暗号化条件を設定することができ、暗号化条件により通信データを暗号化するか否か判定することができる。

【0126】また、この発明によれば、通信相手となる通信装置により暗号化するか否かを設定することができる。

【0127】また、この発明によれば、アプリケーション毎に暗号化するか否かを設定することができる。

【0128】また、この発明によれば、通信方向により暗号化するか否かを設定することができる。

【0129】また、この発明によれば、複数あるセッション鍵の中から暗号化条件に定められたセッション鍵で暗号化、あるいは、復号することができる。また、グループ化された通信装置による暗号グループと平行して暗号グループと異なるセッション鍵によるグループを形成することができる。

【0130】また、この発明によれば、鍵管理装置においてグループ毎に個別のセッション鍵を生成することができる。

【0131】また、この発明によれば、暗号装置で設定されたモードスイッチを有効とするか無効とするかを鍵管理装置から管理することができる。

【0132】また、この発明によれば、鍵管理装置から各暗号装置の暗号化条件を設定することができるため、鍵管理装置において暗号化条件の一括管理ができる。

【0133】また、この発明によれば、鍵管理装置で生成したセッション鍵を暗号化し、グループに対応付けられた暗号装置に配送することができるため、セッション鍵の設置が自動的にできる。

【0134】また、この発明によれば、複数の暗号管理ドメイン同士で暗号通信を行うことができる。

【0135】また、この発明によれば、暗号化条件により暗号化するか否かを設定することができる。

【0136】また、この発明によれば、暗号化条件を特例バスと基本バスを用いて設定することができる。

【0137】また、この発明によれば、暗号化条件をアプリケーションにより定めることができる。

【0138】また、この発明によれば、暗号化条件を通信方向により定めることができる。

【0139】また、この発明によれば、複数あるセッション鍵の中から任意のセッション鍵を用いて暗号化するか否か定めることができる。

【0140】また、この発明によれば、暗号化条件は、通信相手となる通信装置により設定することができる。

【0141】また、この発明によれば、暗号装置に備えられた1以上のポート毎に基本バスと特例バスを設定することができる。そのため、きめ細かな条件設定ができるので、使い勝手のよい暗号化システムを提供すること

ができる。

【0142】また、この発明によれば、鍵管理装置がポート条件を生成し暗号装置に配布するため、鍵管理装置でポート条件の一括管理ができる。

【図面の簡単な説明】

【図1】 この発明の一実施の形態におけるネットワークシステムを示す図である。

【図2】 この発明の一実施の形態における暗号化システムのブロック図である。

10 【図3】 図2における暗号化システムのセッション鍵の配達手順を示すシーケンス図である。

【図4】 図2における暗号化システムのグループ分けを説明する図である。

【図5】 暗号化システムにおける有効無効情報設定用画面の例を示す図である。

【図6】 K E Y D I S T コマンドに設定される内容を示す図である。

【図7】 図2における有効無効判定手段の論理積の結果を説明する図である。

20 【図8】 図4におけるモードスイッチの切り換えと有効無効情報設定後の平文通信での通信データの流れを示す図である。

【図9】 図2における暗号化システムの他の構成を示すブロック図である。

【図10】 図2における暗号化システムの他の構成を示すブロック図である。

【図11】 この発明の一実施の形態における暗号化システムのブロック図である。

【図12】 図11における暗号化システムのネットワーク例を示す図である。

30 【図13】 図11における暗号化システムのネットワーク例を示す図である。

【図14】 図11における暗号化システムのネットワーク例を示す図である。

【図15】 図11における暗号化システムのネットワーク例を示す図である。

【図16】 図11における暗号化システムの論理グループを説明するための図である。

40 【図17】 図11における暗号化システムの他の構成例を示すブロック図である。

【図18】 図11における暗号化システムの他の構成例を示すブロック図である。

【図19】 この発明の一実施の形態におけるネットワークシステムを示す図である。

【図20】 N O D E 型暗号装置を示す図である。

【図21】 H U B 型暗号装置を示す図である。

【図22】 この発明の一実施の形態における暗号化システムのブロック図である。

50 【図23】 図22における暗号化条件記憶手段に記憶する暗号化条件の例を示す図である。

【図24】 図22におけるポート条件記憶手段に記憶するポート条件の例を示す図である。

【図25】 図24に示したポート条件における基本バスと特例バスの関係を説明する図である。

【図26】 図19に示したネットワークシステムにおいて形成される新たなグループを示す図である。

【図27】 HUB型暗号装置を用いた通信形態の例を示す図である。

【図28】 図27における通信端末22のポート条件の設定を説明する図である。

【図29】 LANに接続する暗号装置の図である。

【図30】 LANに接続する暗号装置の第1の設置例を示す図である。

【図31】 LANに接続する暗号装置の第2の設置例を示す図である。

【図32】 LANに接続する暗号装置を用いた通信形態を示す図である。

【図33】 図32に示した暗号装置503における暗号条件を説明する図である。

【図34】 この発明の一実施の形態におけるネットワークシステムを示す図である。

【図35】 この発明の一実施の形態における鍵管理装置のブロック図である。

【図36】 図35に示すセッション鍵テーブルを示す図である。

【図37】 図34に示すネットワークシステムにおいて暗号管理ドメインを超えたグループの例を示す図である。

【図38】 従来の暗号通信システムを示す構成図である。

【図39】 図38におけるセッション鍵問い合わせ手段の詳細な構成を示す構成図である。

【図40】 従来の暗号通信システムにおけるセッショ

ン鍵の配達の手順を示すシーケンス図である。

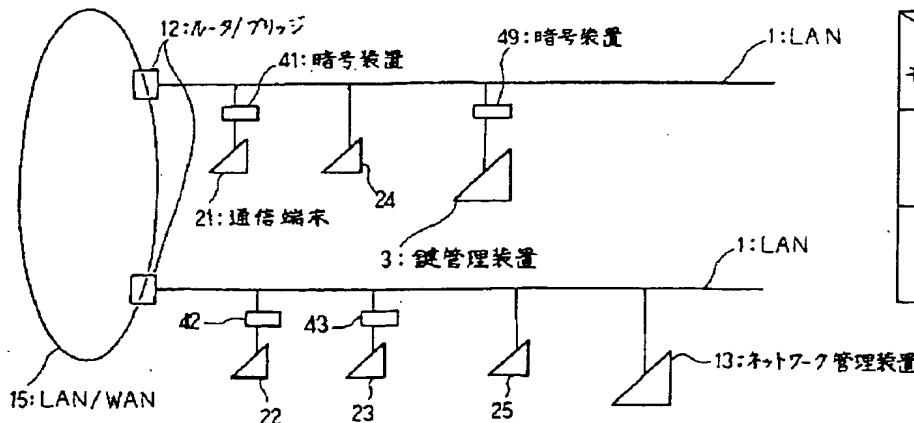
【符号の説明】

1 LAN, 3, 3a, 6, 6a, 7, 71, 72, 73 鍵管理装置, 5 入出力装置, 1-2 ルータ/ブリッジ, 13 ネットワーク管理装置, 14, 141~146 ルータ, 15 LAN/WAN, 16 インターネット, 17 WAN, 20~29, 2a~2m 通信端末, 31 セッション鍵生成手段, 32 セッション鍵管理手段, 33 セッション鍵送信開始検出手段, 34

10 セッション鍵暗号化手段, 35 セッション鍵送信手段, 37 通信装置グループ記憶手段, 41, 41a, 41b, 42a, 42b, 43~46, 49, 51~54, 81, 81a, 81b, 82, 82a, 82b, 83~88, 501~503 暗号装置, 61 有効無効設定手段, 62 暗号化条件設定手段, 63 ポート条件設定手段, 64 セッション鍵テーブル, 65 セッション鍵受信手段, 66 セッション鍵復号手段, 91 サーバ, 92 WWW代理サーバ, 93 WWW, 94 メールサーバ, 95, 903 WWWサーバ, 96

20 メールサーバA, 97, 98 社内メールサーバ, 99 人事ファイルサーバ, 121, 122 一般HUB, 131, 132 イーサネット・スイッチ, 151 ブリッジ, 211, 221 アプリケーション, 212, 222 通信制御手段, 411, 421 セッション鍵復号手段, 412, 422 セッション鍵受信手段, 413, 423 暗号処理手段, 414, 424 データ送受信手段, 711, 721 セッション鍵記憶手段, 712, 722 モードスイッチ, 713, 723 有効無効判定手段, 811, 821 暗号化条件記憶手段, 812, 822 条件判定手段, 901 EOAサーバ, 902 ニュースサーバ, 904, 905 DBサーバ。

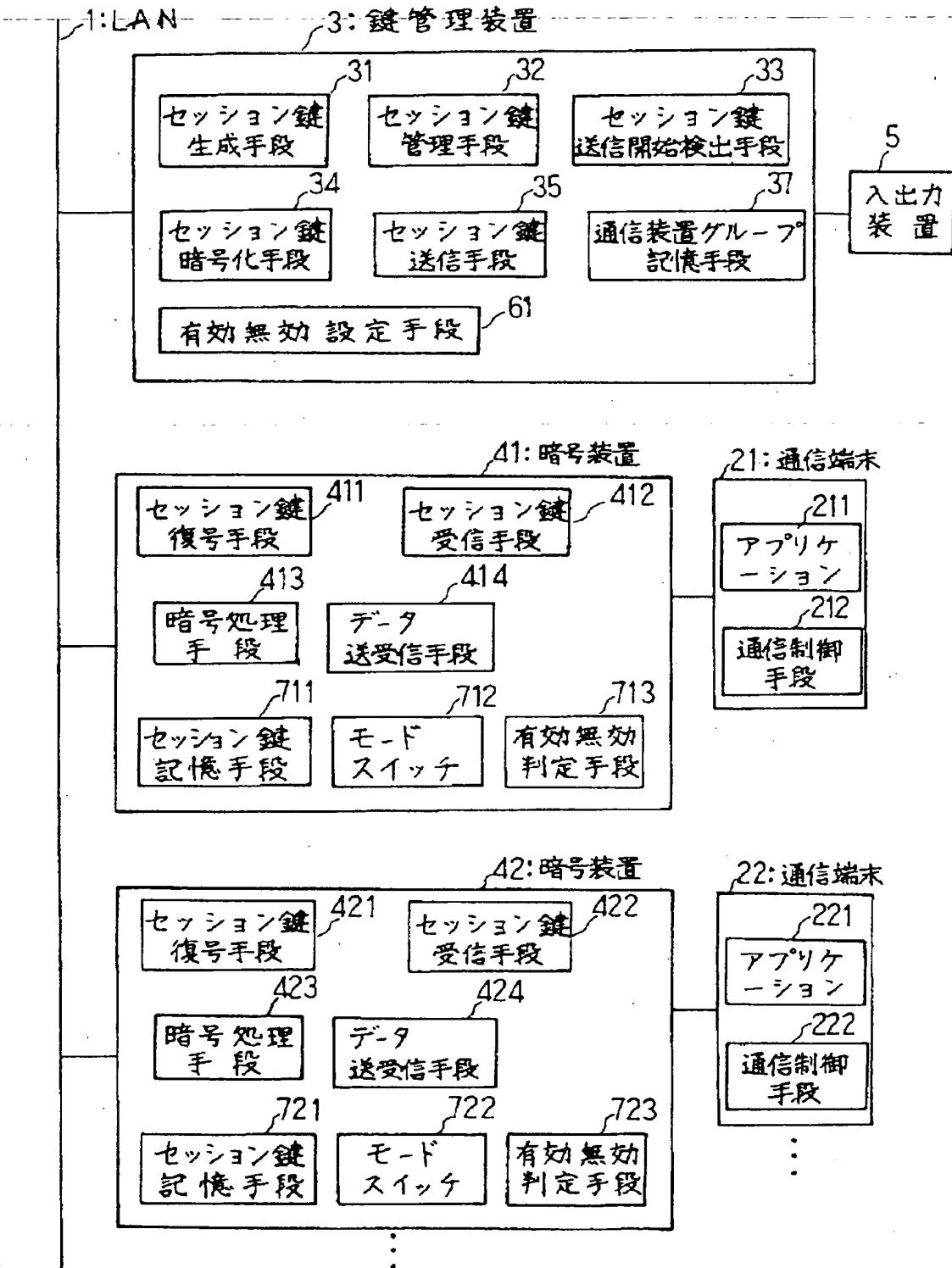
【図1】



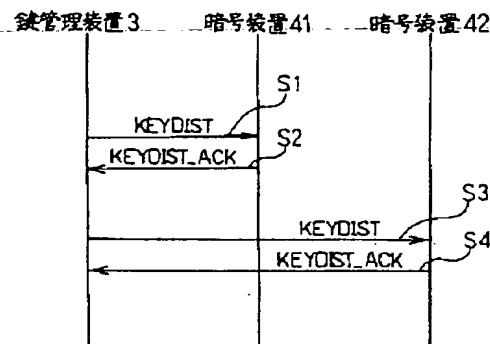
【図7】

モード スイッチ	有効	無効
	有効(1)	無効(0)
OFF (0)	暗号(0)	暗号(0)
ON (1)	透過(1)	暗号(0)

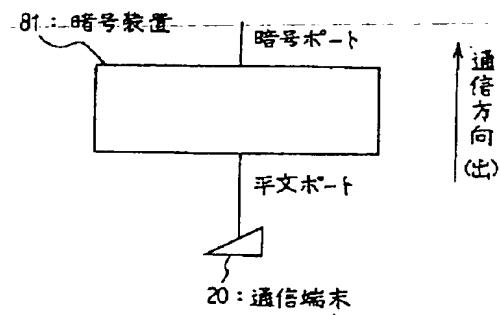
[図 2]



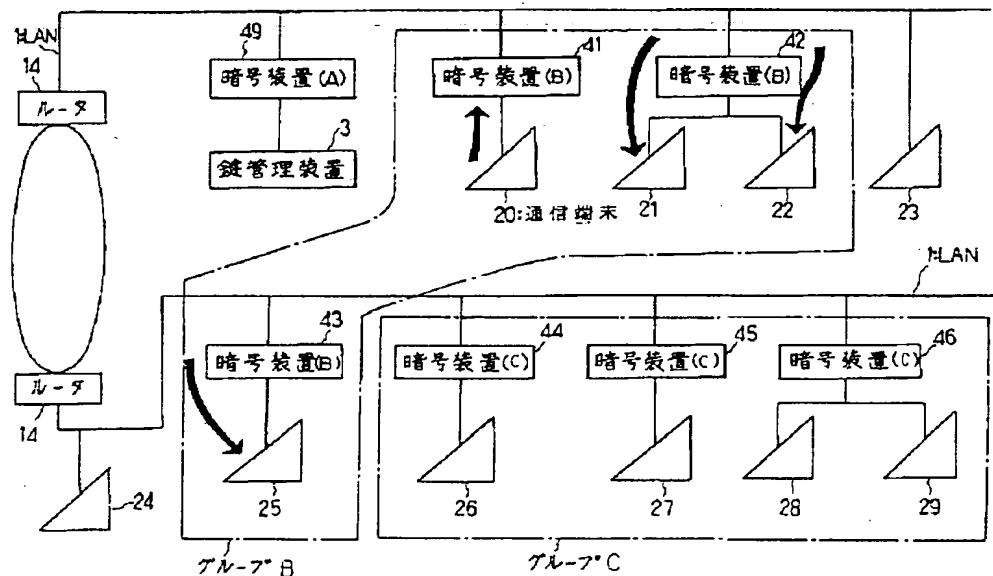
【図 3】



【図 20】



【図 4】

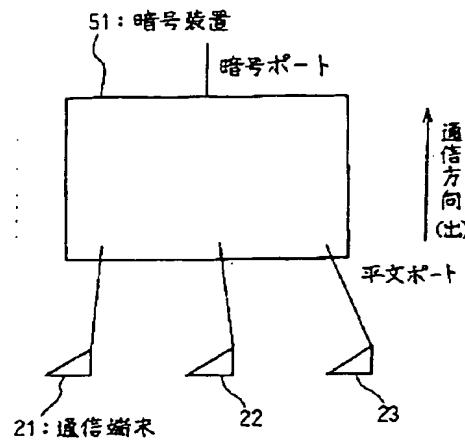


【図 5】

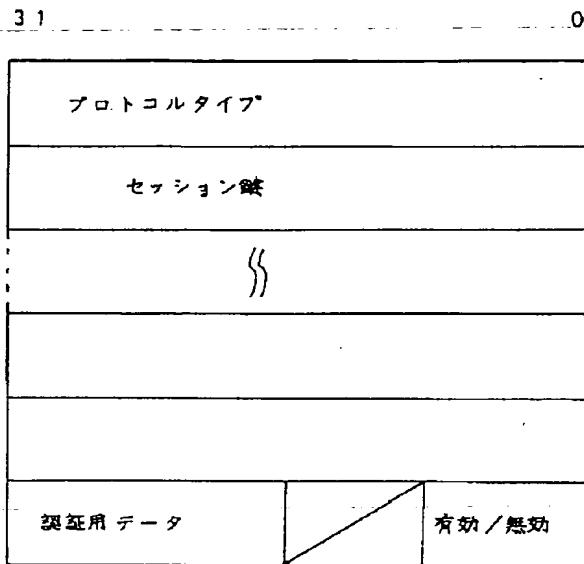
グループ名	GN	IPアドレス	備考	有効/無効
鍵管理装置	A	aaa.aaa.aaa.aaa	管理室	無効
人事部	B	aaa.aaa.aaa.bbb	人事 1 G	有効
人事部	B	aaa.aaa.aaa.ccc	人事 1 G	無効
人事部	B	aaa.aaa.aaa.ddd	人事 2 G	無効
経理部	C	aaa.aaa.aaa.eee	経理 1 G	無効
経理部	C	aaa.aaa.aaa.fff	経理 2 G	無効
経理部	C	aaa.aaa.aaa.ggg	経理 3 G	有効 0 0

Input field: 入力フィールド

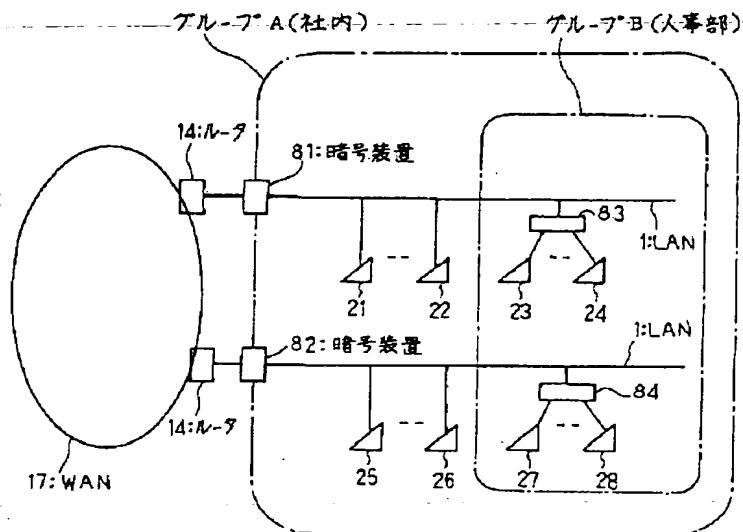
【図 21】



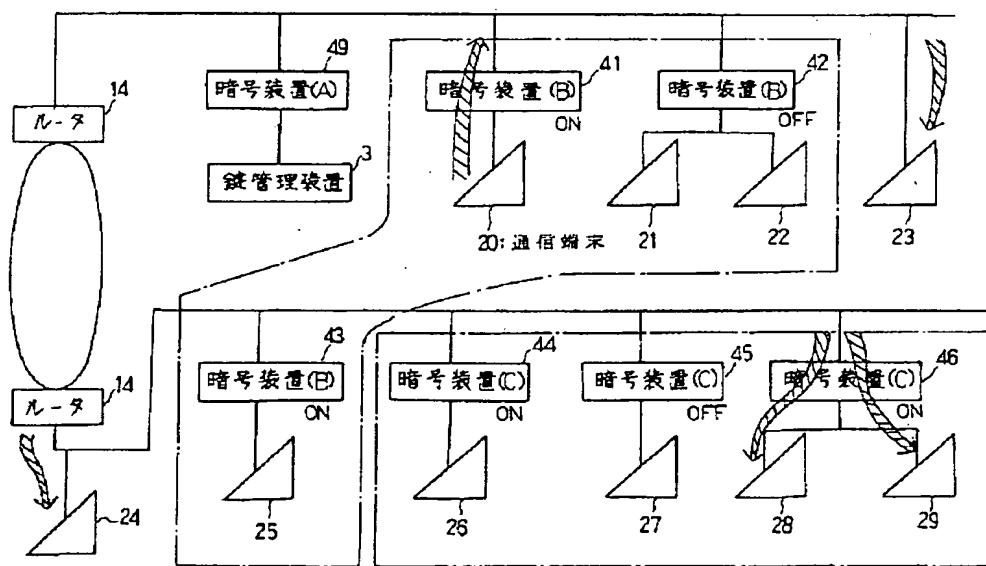
【図 6】



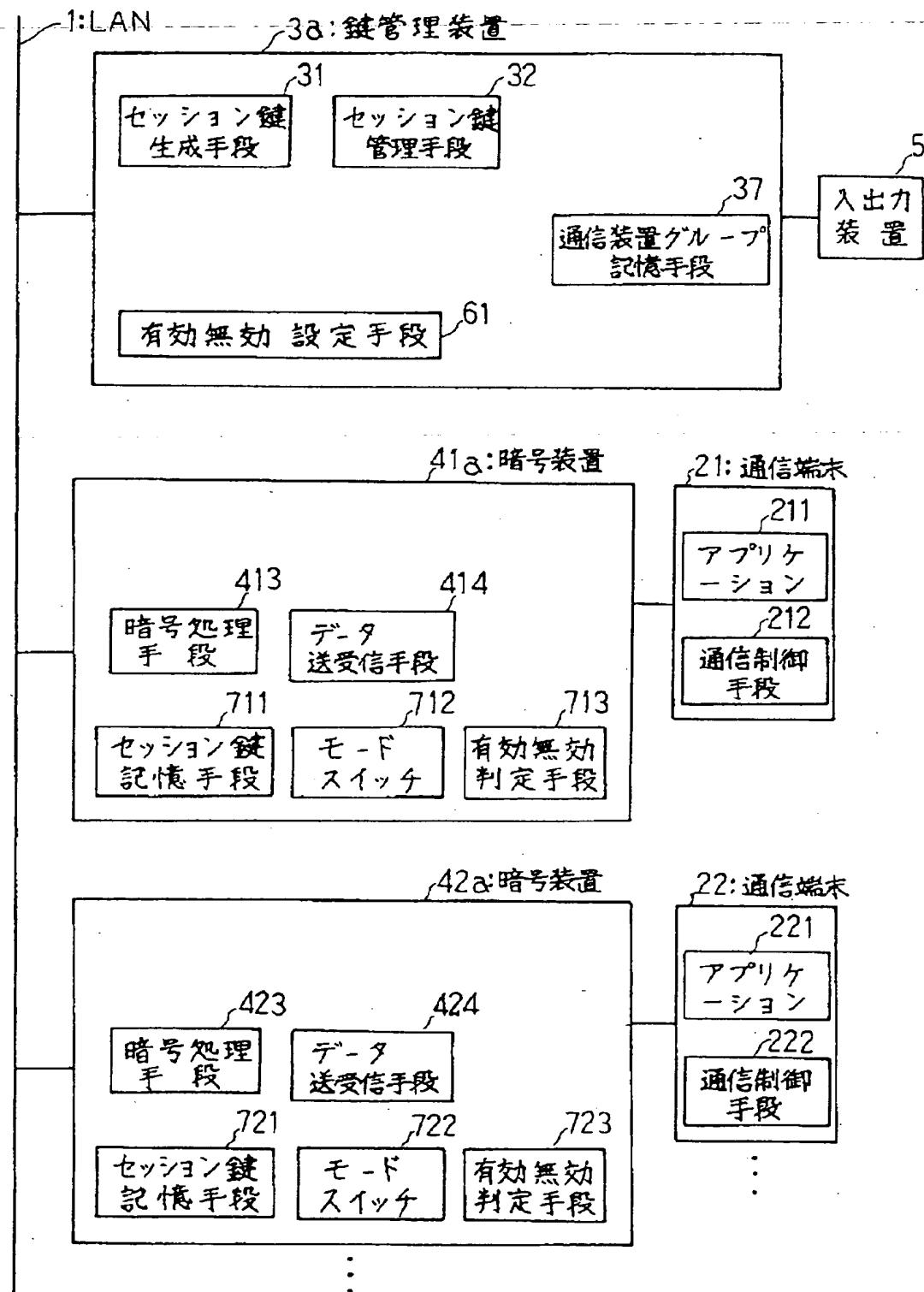
【図 15】



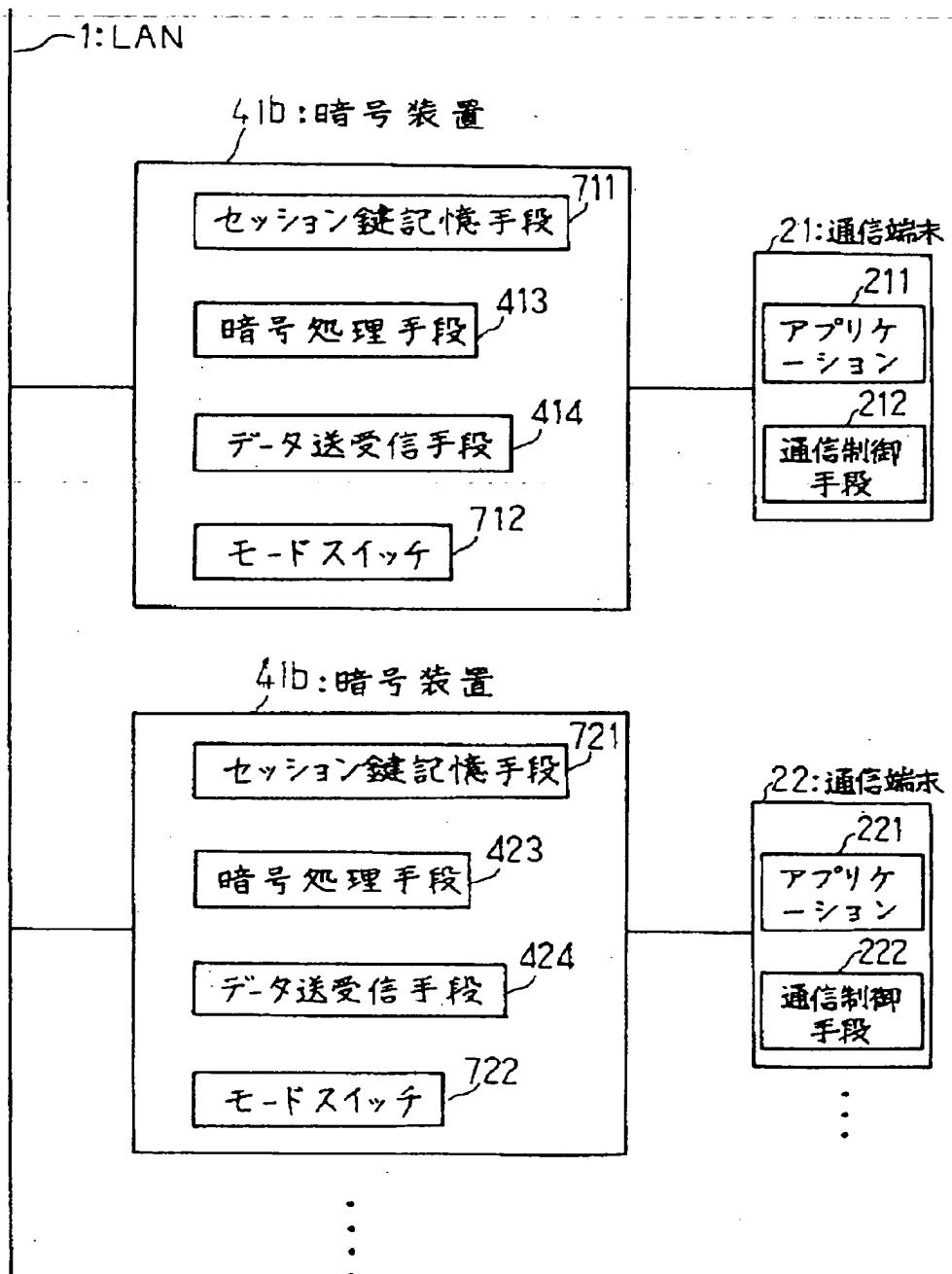
【図 8】



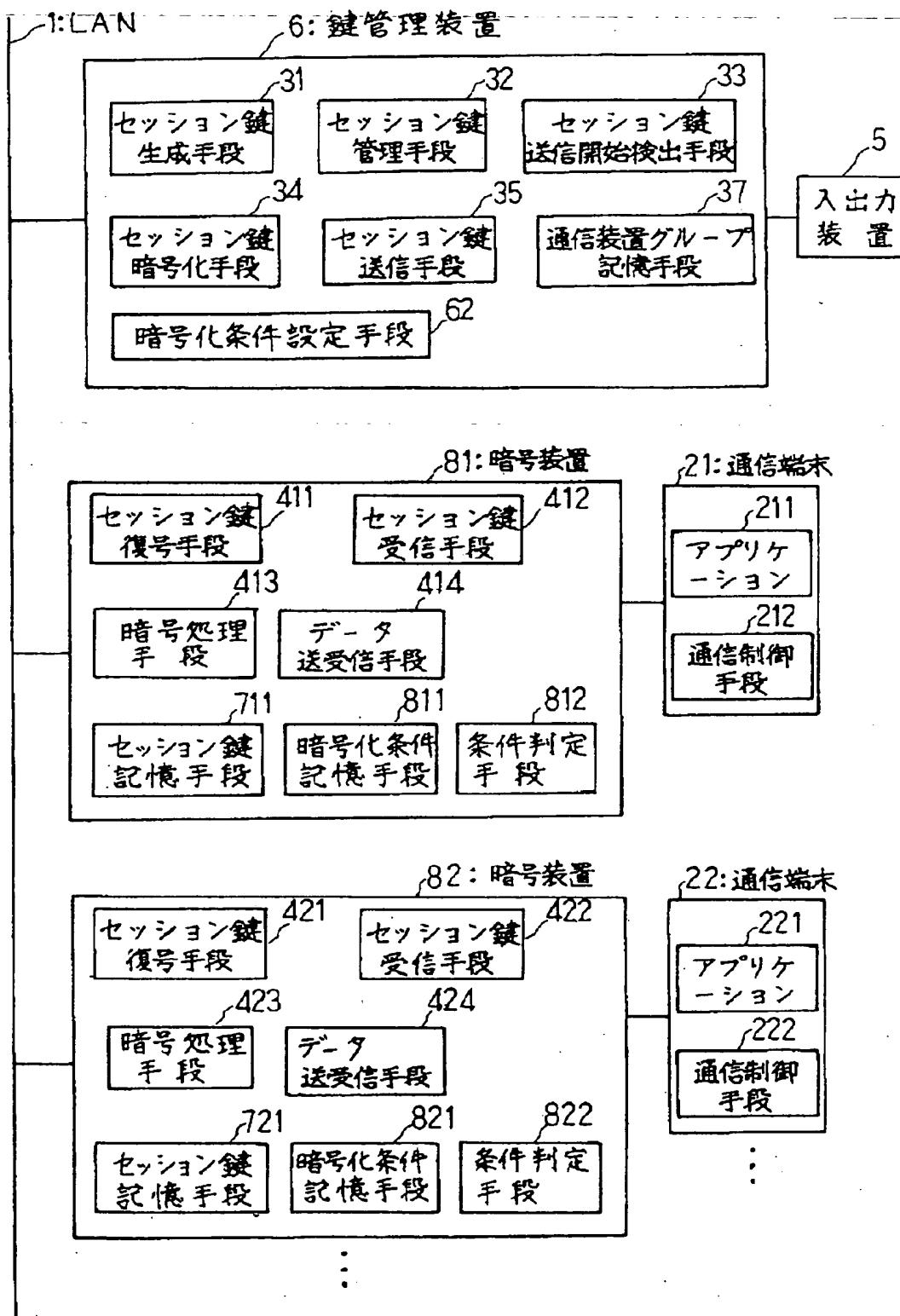
【図 9】



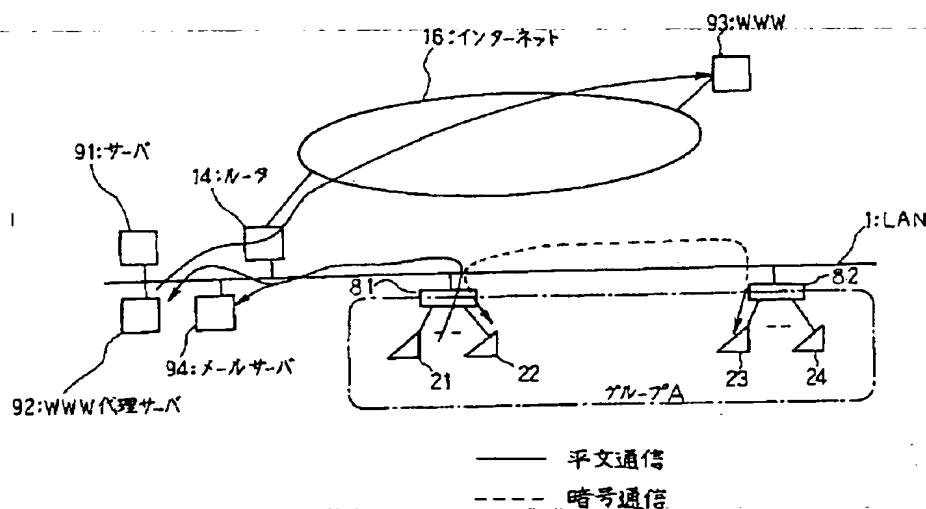
【図 10】



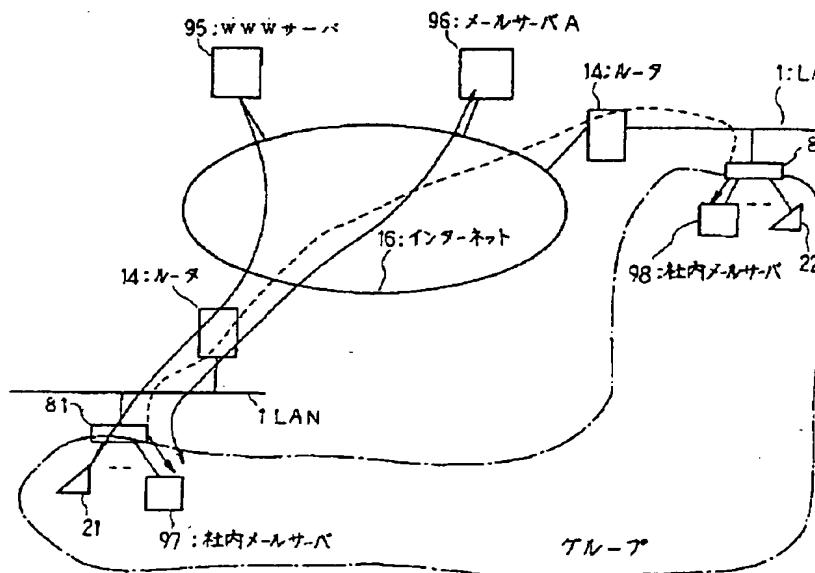
【図 11】



【図 1 2】



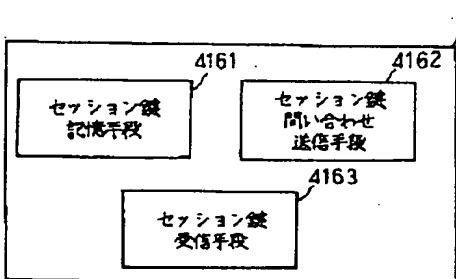
【図 1 3】



【図 3 6】

鍵番号	許可 フラグ	鍵	属性
1	0	ローカル鍵 1	
2	0	ローカル鍵 2	
3	0	ローカル鍵 3	
4	0	ローカル鍵 4	
5	X	共通鍵 1	共通(A,B)
⋮	⋮	⋮	
8	X	共通鍵 2	共通(A,B)
⋮	⋮	⋮	
30	0	ローカル鍵 28	
31	0	ローカル鍵 29	
32	X	共通鍵 3	共通(A,B)

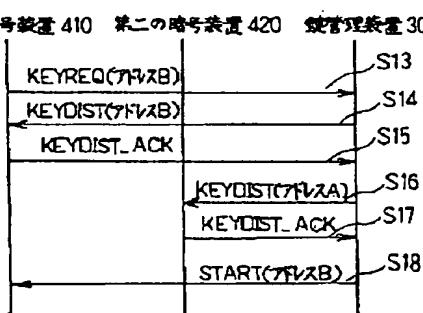
【図 3 9】



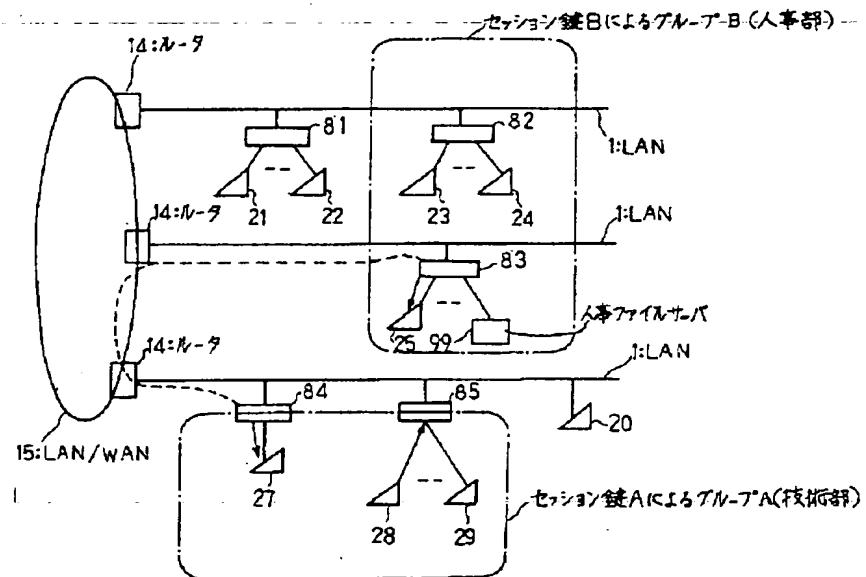
4160: セッション鍵問い合わせ手段

4161 セッション鍵
交換手段4162 セッション鍵
問い合わせ
送信手段4163 セッション鍵
受信手段

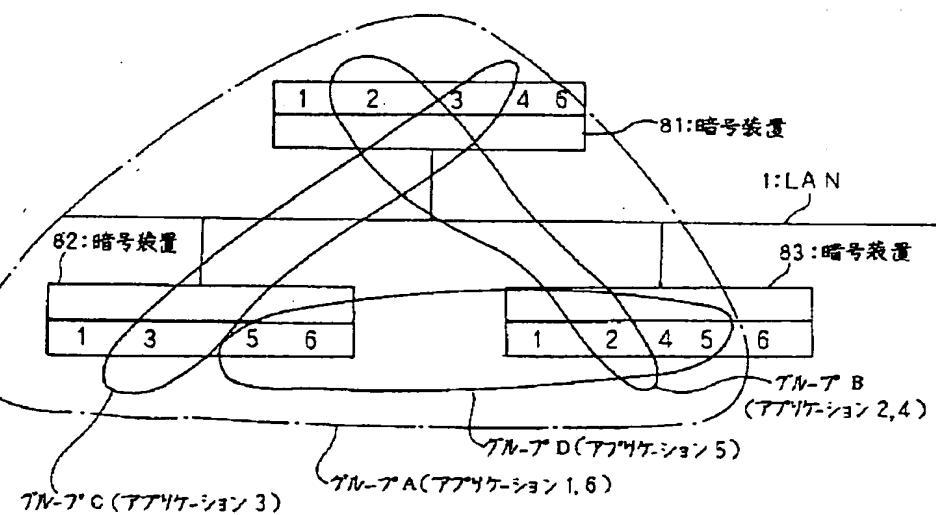
【図 4 0】



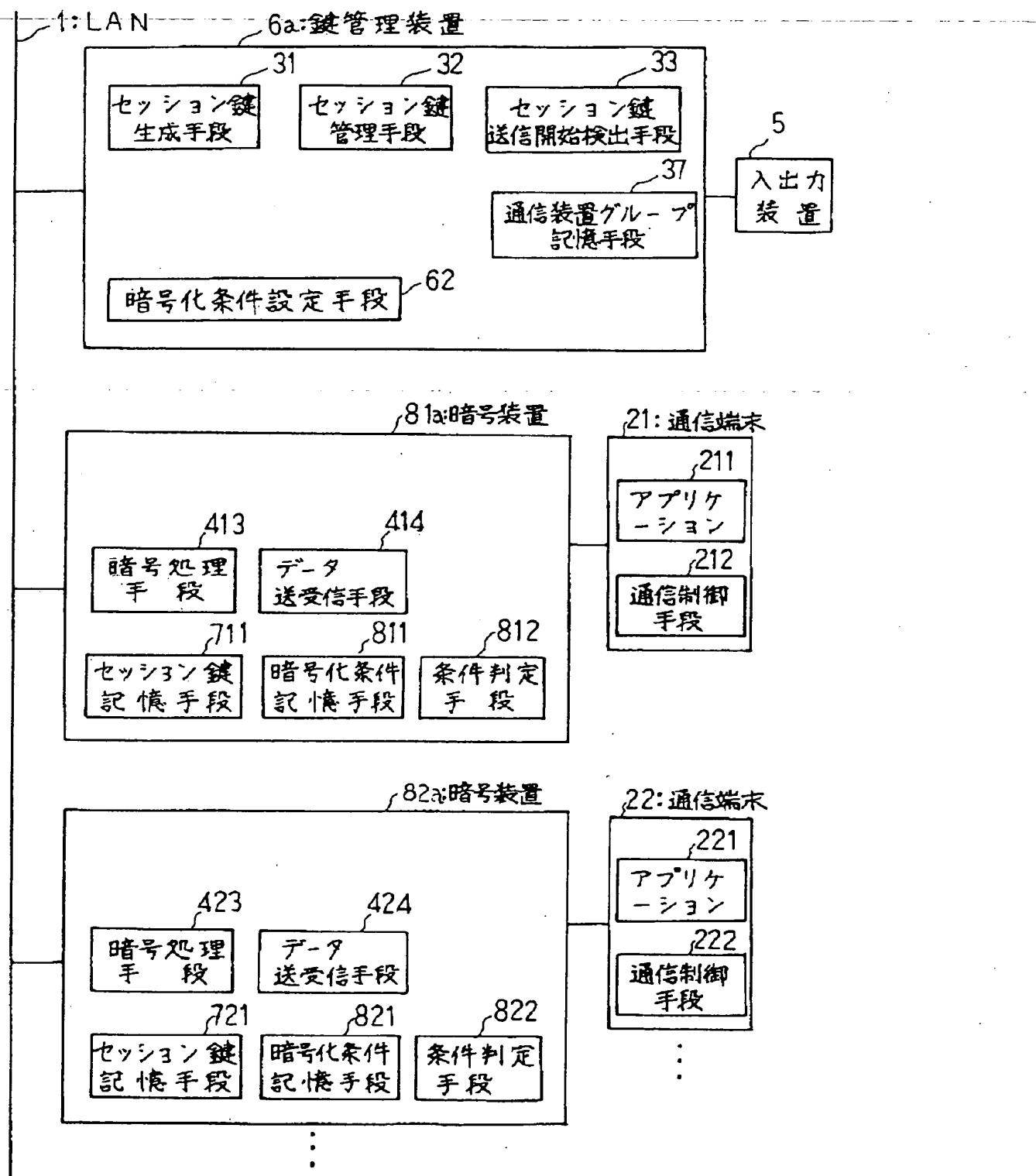
【図 1 4】



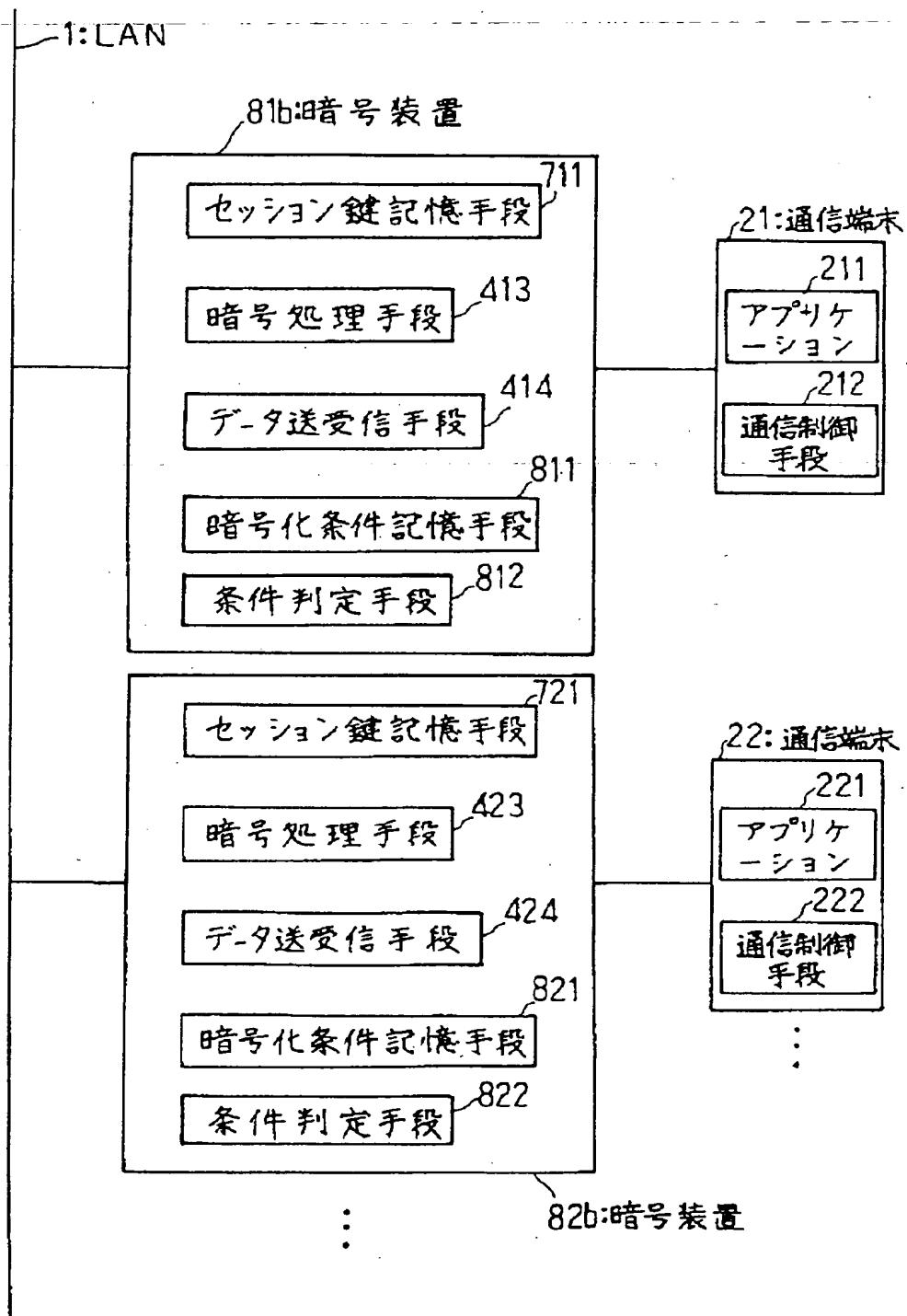
【図 1 6】



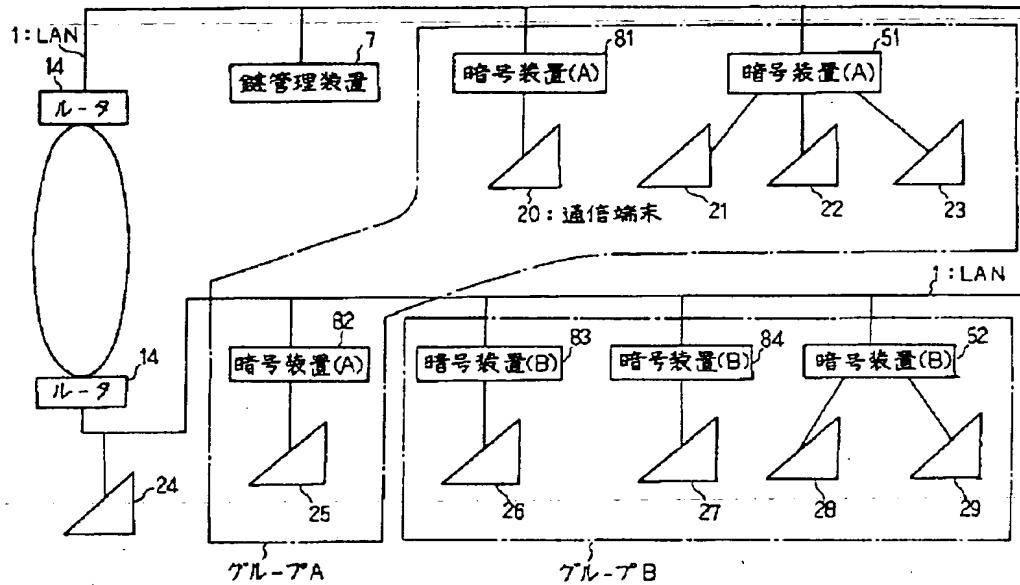
【図 17】



〔図 18 〕



【図19】



【図23】

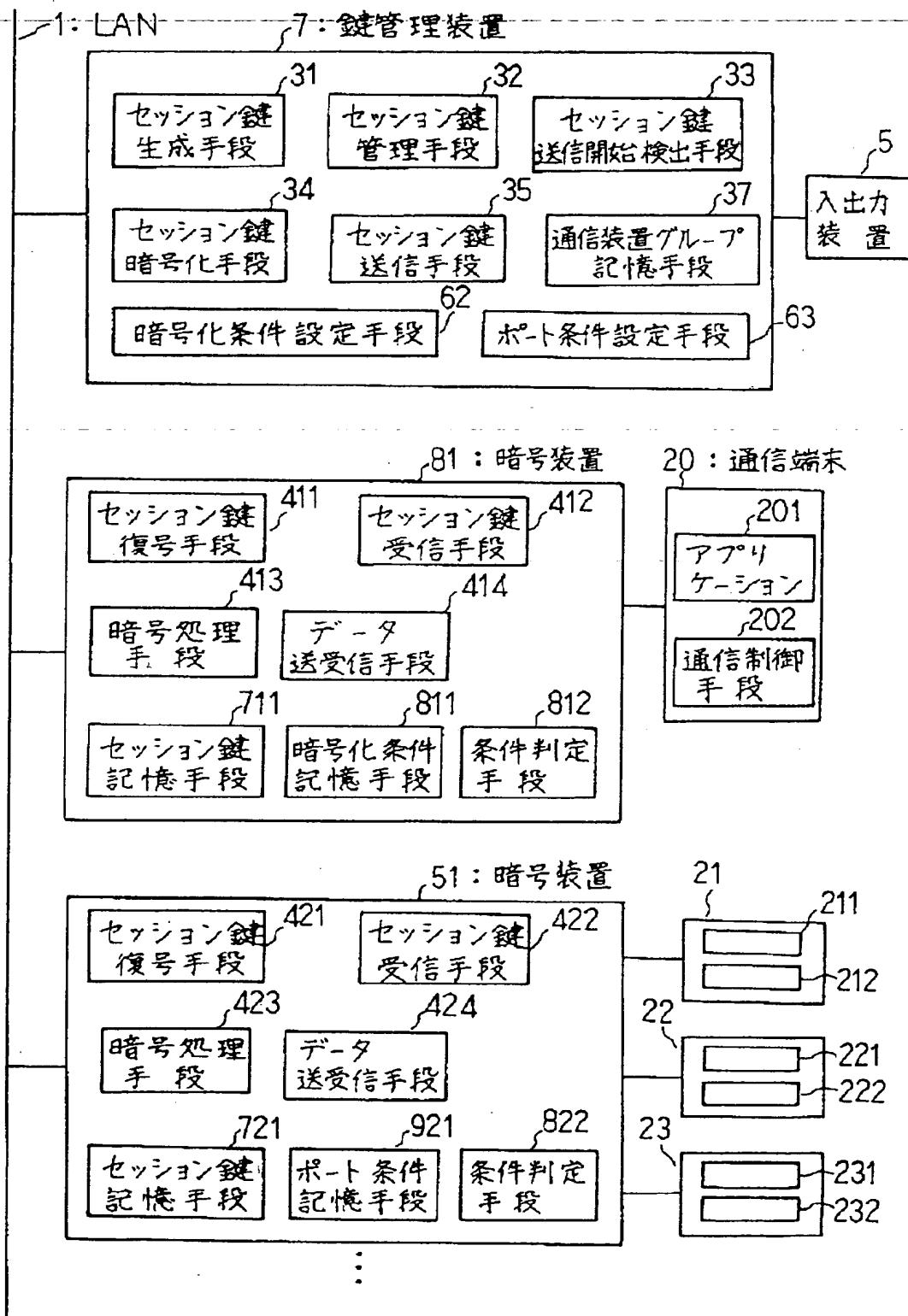
基本バス1: アプリケーション(全), 鍵A
 特例バス0: 宛先IPアドレス(全)
 &
 アプリケーション(メール), 透過
 特例バス1: 宛先IPアドレス(通信端末26)
 &
 アプリケーション(AP11)
 &
 通信方向(出), 鍵B

811: 暗号化条件記憶手段

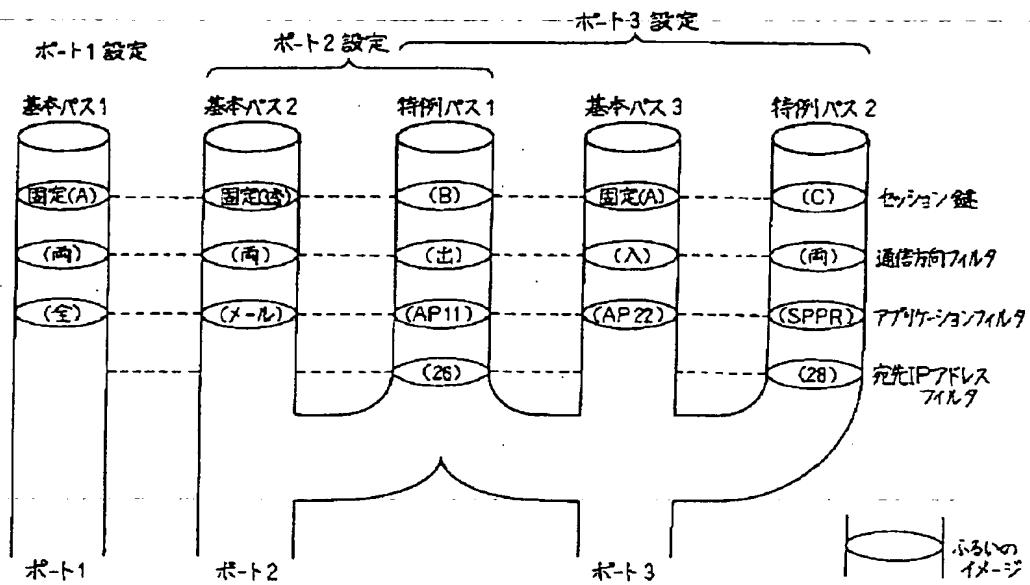
ポート1
 基本バス1: アプリケーション(全), 鍵A
 ポート2
 基本バス2: アプリケーション(メール), 透過
 特例バス1: 宛先IPアドレス(通信端末26)
 & アプリケーション(AP11)&通信方向(出), 鍵B
 ポート3
 基本バス3: アプリケーション(AP22)
 & 通信方向(入), 鍵A
 特例バス1: 宛先IPアドレス(通信端末26)
 & アプリケーション(AP11)&通信方向(出), 鍵B
 特例バス2: 宛先IPアドレス(通信端末28)
 & アプリケーション(SPPR), 鍵C

921: ポート条件記憶手段

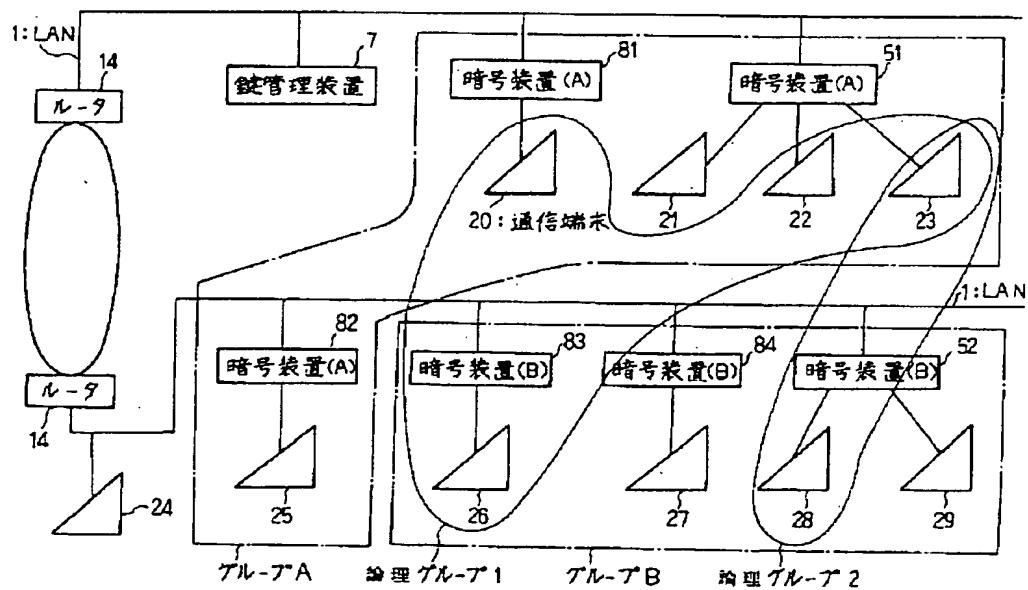
【図 22】



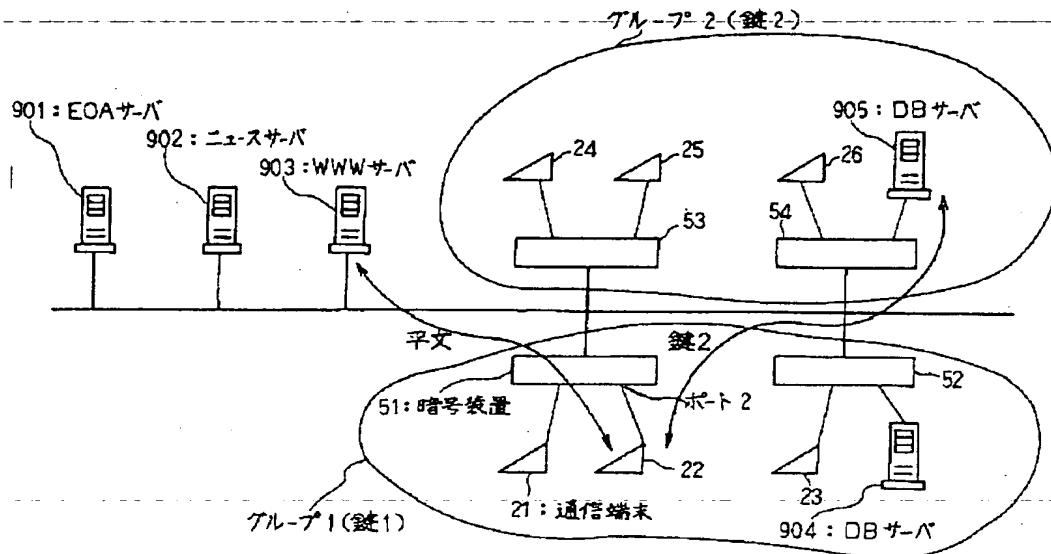
【図 25】



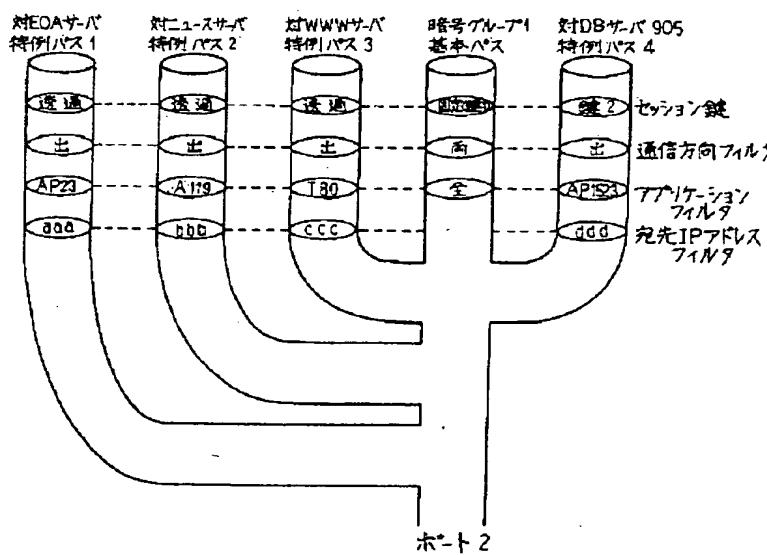
【図 26】



【図 27】

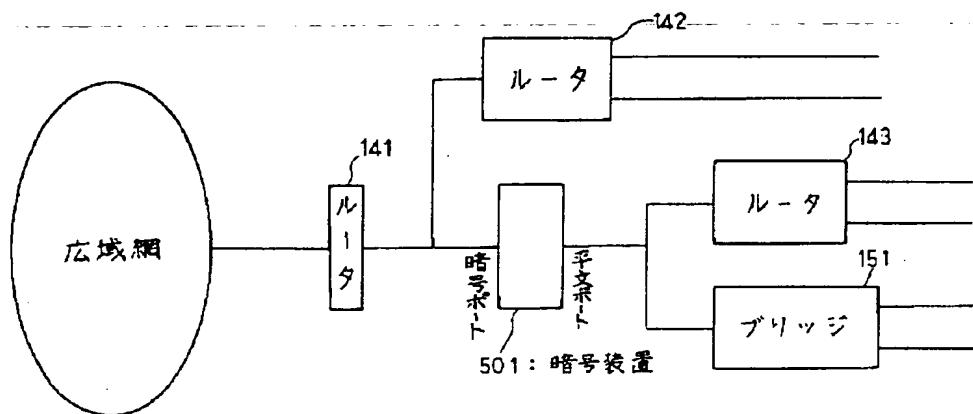


【図 28】



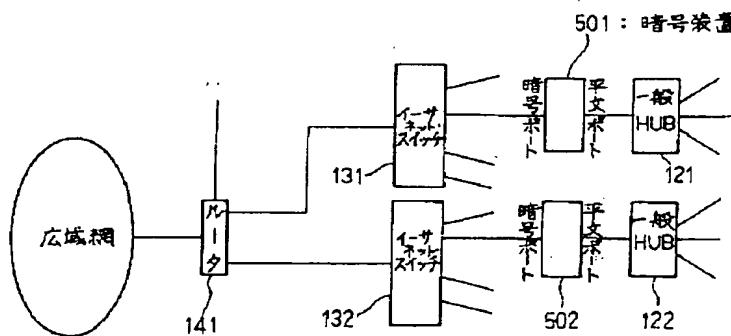
【図 29】

【図 3 0】



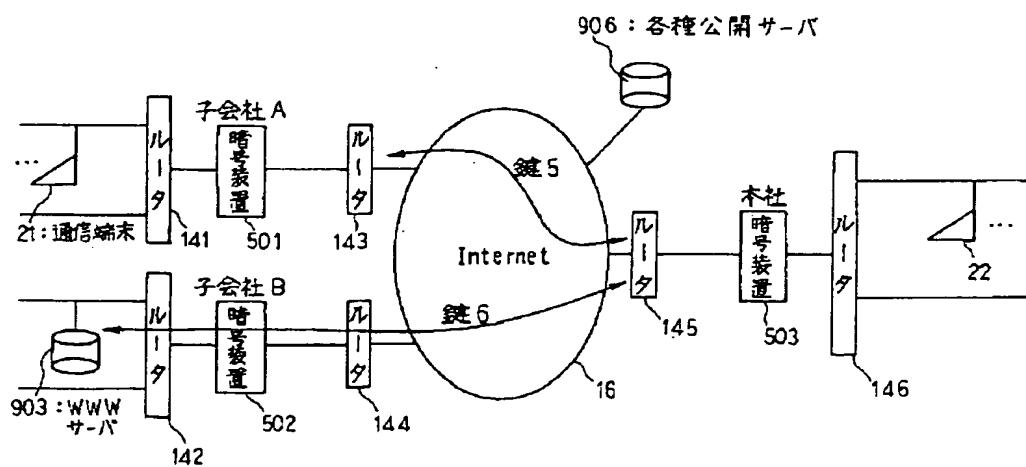
設置例 1

【図 3 1】

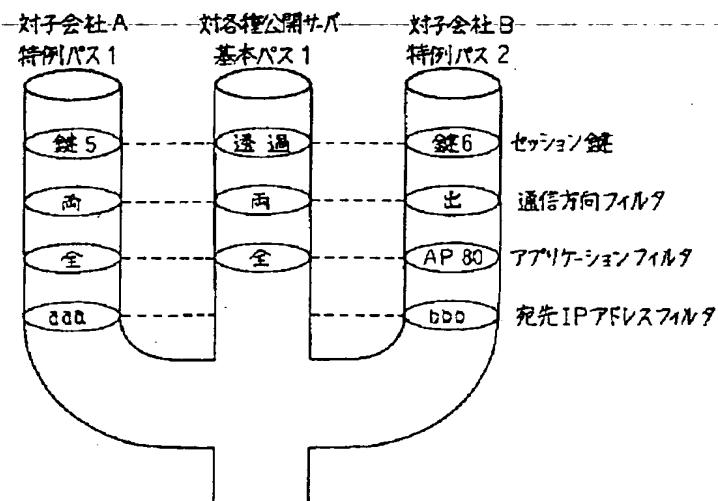


設置例 2

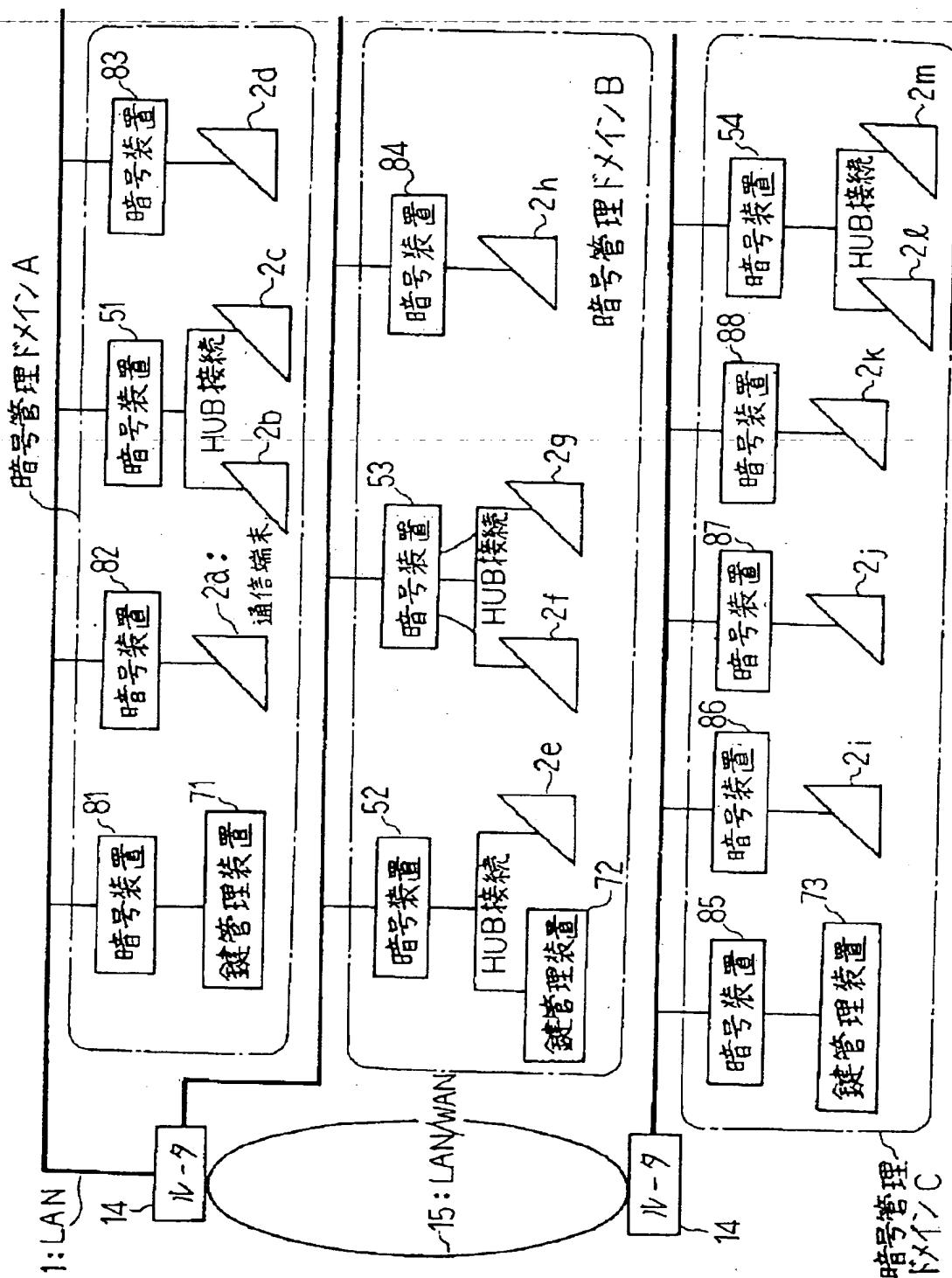
【図 3 2】



【図 33】

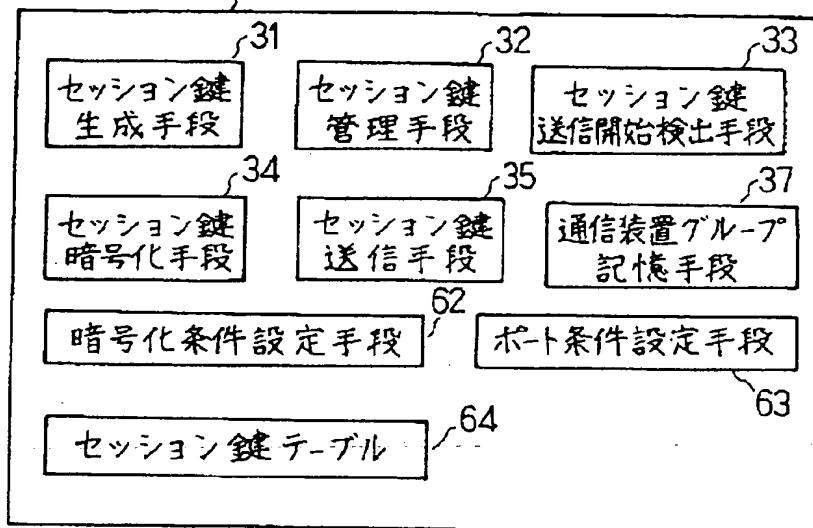


[図 34]

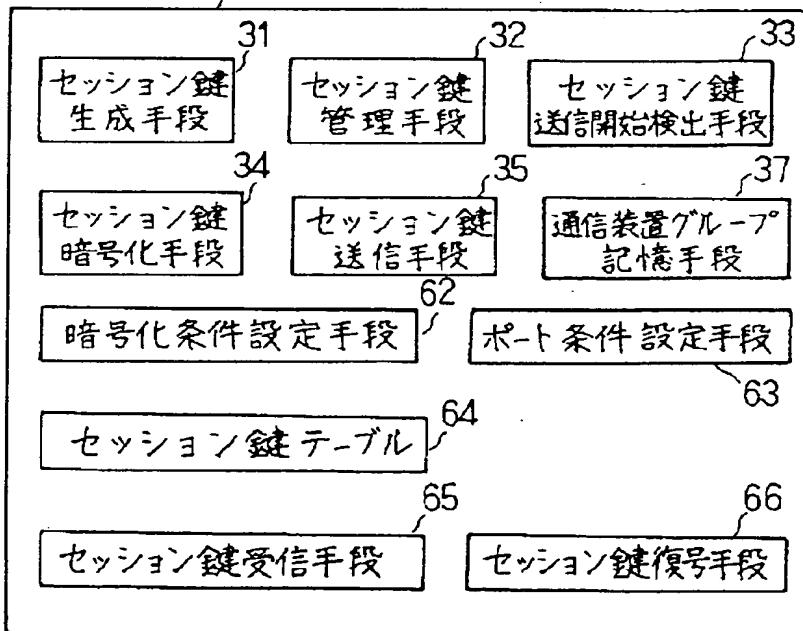


【図 35】

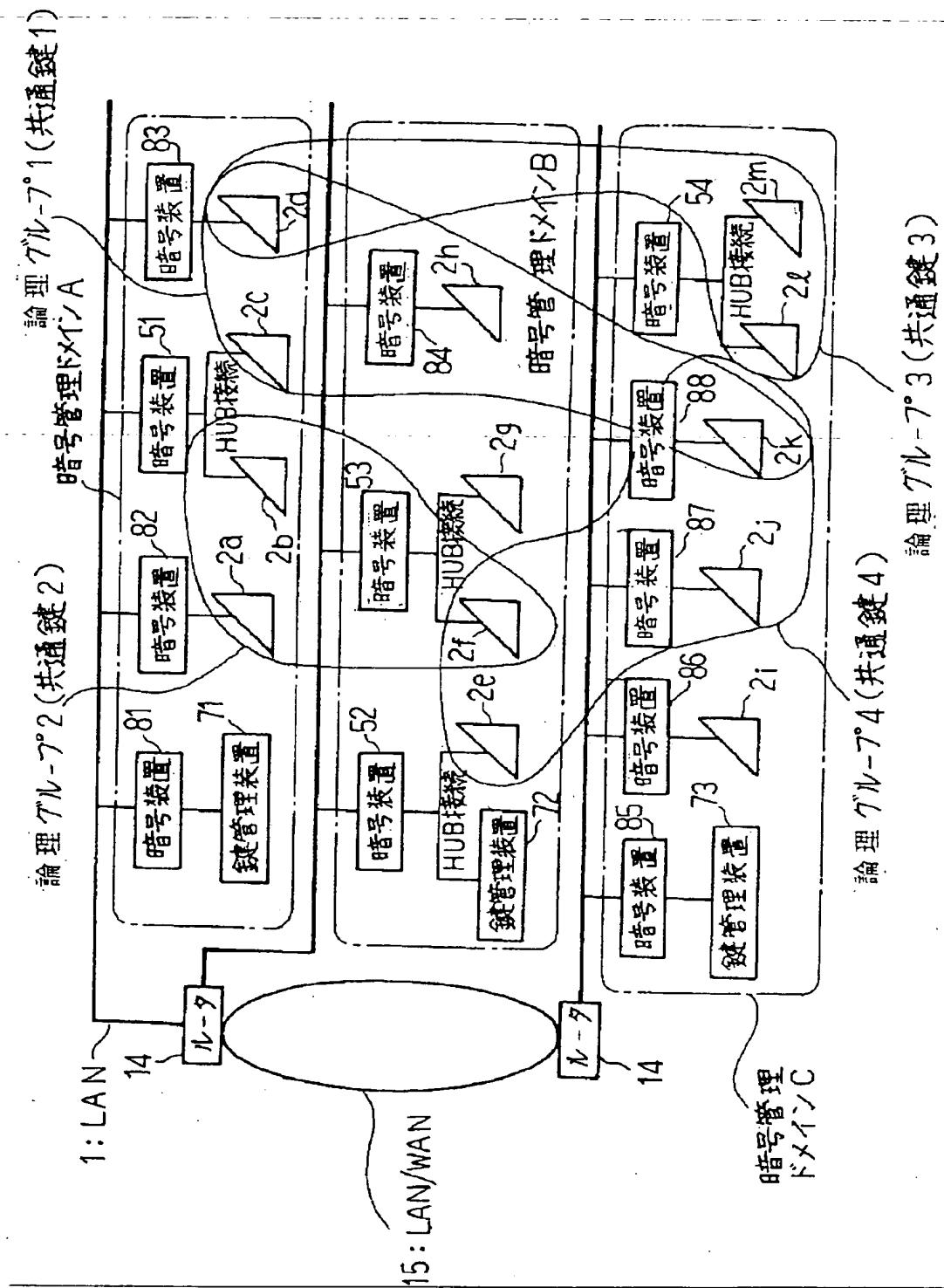
71: 鍵管理装置



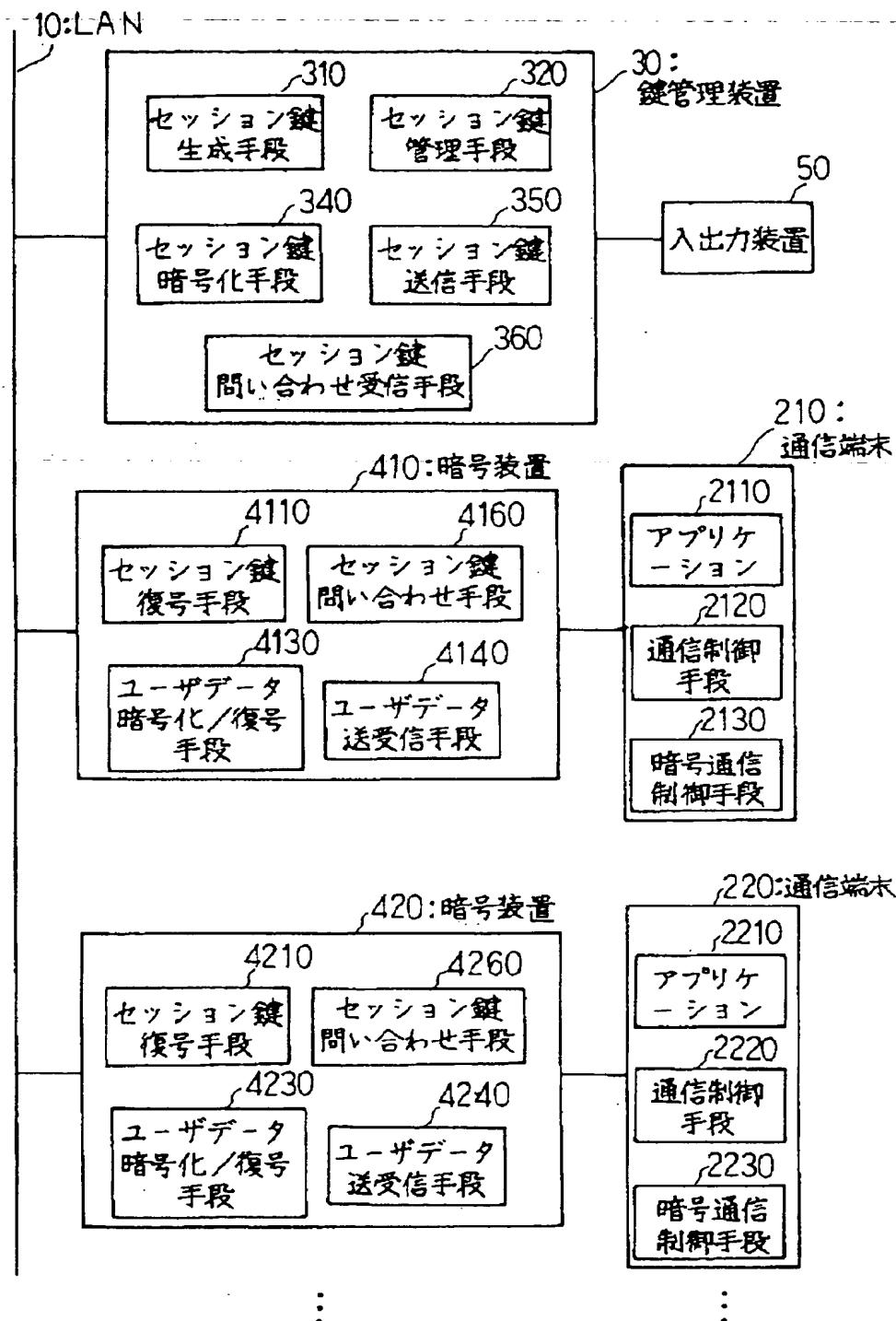
72: 鍵管理装置



[図 37]



【図 38】



【手続補正書】

【提出日】 平成 9 年 3 月 26 日

【手続補正 1】

【補正対象書類名】 明細書

【補正対象項目名】 全文

【補正方法】 変更

【補正内容】

【書類名】 明細書

【発明の名称】 暗号化システム

【特許請求の範囲】

【請求項 1】 グループ化された複数の通信装置と、少なくとも上記複数の通信装置の 1 つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも 1 つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えた暗号化システム。

【請求項 2】 上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも 1 つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする請求項 1 記載の暗号化システム。

【請求項 3】 上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする請求項 1 記載の暗号化システム。

【請求項 4】 上記暗号化条件は、通信相手となる 1 以上の通信装置により定まることを特徴とする請求項 3 記載の暗号化システム。

【請求項 5】 上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする請求項 3 又は 4 いずれかに記載の暗号化システム。

【請求項 6】 上記暗号化条件は、通信方向により定まることを特徴とする請求項 3 から 5 いずれかに記載の暗号化システム。

【請求項 7】 上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする請求項 3 から 6 いずれかに記載の暗号化システム。

【請求項 8】 上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段

と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする請求項 1 から 7 いずれかに記載の暗号化システム。

【請求項 9】 上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、

上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする請求項 8 記載の暗号化システム。

【請求項 10】 上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする請求項 8 記載の暗号化システム。

【請求項 11】 上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、

上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする請求項 8 から 10 いずれかに記載の暗号化システム。

【請求項 12】 複数の鍵管理装置を備え、各鍵管理装置と 1 以上の暗号装置と 1 以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、

上記複数の鍵管理装置の中の 1 台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする暗号化システム。

【請求項 13】 上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも 1 つ記憶するセッション鍵記憶手段と、

上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、

上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、

通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、

上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、上記鍵管理装置は、更に、

上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、

上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする請求項12記載の暗号化システム。

【請求項14】 上記暗号化条件は、特定の通信に関する暗号化条件を設定した1以上の特例バスと上記特例バスに合致しない全ての通信に対する暗号化条件を設定した基本バスとからなることを特徴とする請求項3又は13記載の暗号化システム。

【請求項15】 上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まるることを特徴とする請求項13又は14いずれかに記載の暗号化システム。

【請求項16】 上記暗号化条件は、通信方向により定まることを特徴とする請求項13から15いずれかに記載の暗号化システム。

【請求項17】 上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする請求項13から16いずれかに記載の暗号化システム。

【請求項18】 上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする請求項13から17いずれかに記載の暗号化システム。

【請求項19】 上記暗号装置は、通信装置あるいは鍵管理装置を接続する1以上のポートを備え、ポート毎に上記基本バスと上記特例バスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする請求項14から18いずれかに記載の暗号化システム。

【請求項20】 上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする請求項19に記載の暗号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、通信網における暗号通信に関するものである。

【0002】

【従来の技術】 従来の暗号通信システムとして、例えば、社団法人電子情報通信学会発行の信学技報OFS-38(1994-3)P7~P12「LAN暗号通信方式の実装と評価」に示されるような通信端末及び鍵管理ワークステーション内に暗号通信ボードを置き、ローカルエリアネットワーク(以下LANとする)に接続する構成のシステムがある。図3-8は、このような従来の暗

号通信システムを示す構成図である。図において、10はLAN、210, 220はこのLAN10に暗号装置410, 420を介して接続された通信端末、30は鍵管理装置である。なお、図示していないが、通常は、更に多くの通信端末及び暗号装置が接続されている。

【0003】 通信端末210, 220は、それぞれアプリケーション2110, 2210、通信制御手段2120, 2220、暗号通信制御手段2130, 2230により構成される。鍵管理装置30は、セッション鍵生成手段310、セッション鍵管理手段320、セッション鍵暗号化手段340、セッション鍵送信手段350、セッション鍵問い合わせ受信手段360により構成される。また暗号装置410, 420は、それぞれセッション鍵復号手段4110, 4210、ユーザデータ暗号化/復号手段4130, 4230、ユーザデータ送受信手段4140, 4240、セッション鍵問い合わせ手段4160, 4260により構成される。

【0004】 また、図3-9は、上記セッション鍵問い合わせ手段4160の詳細を示す構成図である。4161はセッション鍵記憶手段、4162はセッション鍵問い合わせ送信手段、4163はセッション鍵受信手段である。なお、セッション鍵問い合わせ手段4260も同様の構成である。

【0005】 次に、このような従来の暗号通信システムにおけるデータ通信の手順につき説明する。暗号を用いて端末間で通信を行うには、通信する端末に接続されている暗号装置同士が共通のセッション鍵を持ち、そのセッション鍵によってデータの暗号化/復号を行う。通信する端末に接続されている暗号装置同士が共通のセッション鍵を持つための手順を鍵配達という。

【0006】 暗号通信を行う際には、鍵配達の手順と、実際のユーザデータの送受信の手順が必要である。従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたびに、これに先立って鍵配達の手順を行うものであった。

【0007】 ここでは、通信端末210のアプリケーション2110が、LAN10を介して接続されている通信端末220のアプリケーション2210と通信を行う際の鍵配達の手順につき説明する。以下の説明において、始めに通信を行おうとする通信端末210のアドレスをAとする。また、通信端末220のアドレスをBとする。

【0008】 図4-0は、従来の暗号通信システムにおけるセッション鍵の配達の手順を示すシーケンス図である。通信端末210のアプリケーション2110が、LAN10を介して接続されている通信端末220のアプリケーション2210と通信を行う際には、まずアプリケーション2110が通信制御手段2120を起動する。そして、通信相手の端末である通信端末220のア

ドレス B の情報を通信制御手段 2120 に渡す。通信制御手段 2120 は、通信端末 220 のアドレス B を記憶装置（図示せず）に記憶するとともに、通信端末 220 のアドレス B の情報を暗号通信制御手段 2130 に渡す。

【0009】暗号通信制御手段 2130 は、アドレス B の情報を含む通信開始要求コマンドを暗号装置 410 に送る。通信開始要求コマンドは、暗号装置 410 のセッション鍵問い合わせ手段 4160 のセッション鍵問い合わせ手段 4162 に渡される。セッション鍵問い合わせ手段 4162 は、上記通信開始要求コマンドに含まれるアドレス B の情報を求め、アドレス B の情報を含む鍵配送要求コマンド KEYREQ を生成し、これを LAN10 を介して鍵管理装置 30 に送信する（S13）。また、セッション鍵記憶手段 4161 は、セッション鍵問い合わせ手段 4162 からのアドレス B の情報を記憶する。

【0010】次に、鍵管理装置 30 により受信された鍵配送要求コマンド KEYREQ は、セッション鍵問い合わせ受信手段 360 に渡され、ここで鍵配送要求コマンドの発信元アドレスであるアドレス A を求め、これを鍵配送要求元アドレスとする。また、鍵配送要求コマンド KEYREQ に含まれる情報よりアドレス B を求め、これを通信先アドレスとし、これらをセッション鍵管理手段 320 に渡す。セッション鍵管理手段 320 は、鍵配送要求元アドレスであるアドレス A と通信先アドレスであるアドレス B の組み合わせを、記憶装置（図示せず）に記憶するとともに、セッション鍵生成手段 310 を起動する。

【0011】セッション鍵生成手段 310 は、セッション鍵管理手段 320 により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段 320 に渡す。セッション鍵管理手段 320 は、このセッション鍵を記憶装置に記憶されている鍵配送要求元アドレスであるアドレス A と、通信先アドレスであるアドレス B の組み合わせとの組として記憶装置に記憶するとともに、セッション鍵暗号化手段 340 に渡す。

【0012】セッション鍵暗号化手段 340 は、このセッション鍵を予め設定されているセッション鍵を暗号化する鍵であるマスター鍵（鍵暗号化鍵）により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段 320 に渡す。セッション鍵管理手段 320 は、暗号化セッション鍵と、記憶装置に記憶されている鍵配送要求元アドレスであるアドレス A と、通信先アドレスであるアドレス B の組み合わせをセッション鍵送信手段 350 に渡す。セッション鍵送信手段 350 は、暗号化セッション鍵と、通信先アドレスであるアドレス B の情報を含んだセッション鍵配送コマンド KEYDIST を生成し、これを鍵配送要求元アドレスであるアドレス A の通信端末 210 に接続されている暗号装置 410 に対して送信する（S14）。

0 に対して送信する（S14）。

【0013】暗号装置 410 により受信されたセッション鍵配送コマンド KEYDIST は、セッション鍵問い合わせ手段 4160 のセッション鍵受信手段 4163 に渡される。セッション鍵受信手段 4163 は、セッション鍵配送コマンド KEYDIST より暗号化セッション鍵と通信先アドレスであるアドレス B の情報を求め、通信先アドレスであるアドレス B を記憶装置に記憶するとともに、暗号化セッション鍵をセッション鍵復号手段 4110 に渡す。

【0014】セッション鍵復号手段 4110 は、暗号化セッション鍵を予め設定されているマスター鍵により復号し、その結果をセッション鍵としてセッション鍵受信手段 4163 に渡す。セッション鍵受信手段 4163 は、セッション鍵をセッション鍵記憶手段 4161 に渡す。また、鍵管理装置 30 に対しセッション鍵受信確認コマンド KEYDIST_ACK を送信する（S15）。また、セッション鍵記憶手段 4161 は、記憶装置に記憶されている通信先アドレスであるアドレス B の情報と、該セッション鍵の組を記憶装置に記憶する。

【0015】鍵管理装置 30 により受信されたセッション鍵受信確認コマンド KEYDIST_ACK は、セッション鍵送信手段 350 に渡され、該コマンドの発信元アドレスであるアドレス A を求め、これを鍵配送要求元アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段 320 に渡す。セッション鍵管理手段 320 は、該鍵配送要求元アドレスと記憶装置に記憶されている鍵配送要求元アドレスとを照合する。一致する鍵配送要求元アドレスとの組として記憶されている通信先アドレスであるアドレス B とセッション鍵の内、通信先アドレスであるアドレス B を記憶装置に記憶するとともに、セッション鍵暗号化手段 340 に該セッション鍵を渡す。

【0016】セッション鍵暗号化手段 340 は、該セッション鍵を予め設定されているマスター鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段 320 に渡す。セッション鍵管理手段 320 は、該暗号化セッション鍵と、記憶装置に記憶されている通信先アドレスであるアドレス B の組み合わせをセッション鍵送信手段 350 に渡す。セッション鍵送信手段 350 は、該暗号化セッション鍵と、記憶装置に記憶してある鍵配送要求元アドレスであるアドレス A の情報を含んだセッション鍵配送コマンド KEYDIST を生成する。これを通信先アドレスであるアドレス B の通信端末に接続されている暗号装置である暗号装置 420 に対して送信する（S16）。

【0017】暗号装置 420 では、上記暗号装置 410 と同様の動作が行われ、鍵管理装置 30 に対し、セッション鍵受信確認コマンド KEYDIST_ACK を送信する（S17）。鍵管理装置 30 により受信されたセッ

ション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段350に渡され、該コマンドの発信元アドレスであるアドレスBを求め、これを通信先アドレスとし、これを記憶装置に記憶するとともに、セッション鍵管理手段320に渡す。

【0018】セッション鍵管理手段320は、該通信先アドレスと記憶装置に記憶されている通信先アドレスとを照合し、一致する通信先アドレスとの組として記憶されている鍵配送要求元アドレスであるアドレスAを、セッション鍵送信手段350に渡す。セッション鍵送信手段350は、記憶装置に記憶されている通信先アドレスであるアドレスBの情報を含んだ通信開始コマンドSTARTを生成する。これを鍵配送要求元アドレスであるアドレスAの通信端末に接続されている暗号装置410に対して送信する(S18)。

【0019】暗号装置410により受信された通信開始コマンドSTARTは、ユーザデータ送受信手段4140に渡される。ユーザデータ送受信手段4140は、通信開始コマンドSTARTより通信先アドレスであるアドレスBの情報を求め、これを記憶装置に記憶する。更に、通信端末210に鍵配送確認コマンドを送る。鍵配送確認コマンドは、通信端末210の暗号通信制御手段2130に渡される。暗号通信制御手段2130は、該鍵配送確認コマンドに含まれる通信先アドレスであるアドレスBの情報を求め、これを通信相手アドレスとし、該通信相手アドレスと通信開始フラグをONとした情報との組を、記憶装置に記憶する。また、通信制御手段2120に該通信相手アドレスの情報を含む通信開始通知を渡す。以上の手順に従って、鍵配送が行われることにより、暗号装置410と暗号装置420が共通のセッション鍵を持つことができる。

【0020】次に、通信端末210のアプリケーション2110が、LAN10を介して接続されている通信端末220のアプリケーション2210と、通信を行う際のユーザデータの転送の手順につき詳細に説明する。通信端末210のアプリケーション2110は、ユーザデータと通信端末220のアドレスBとの組を通信制御手段2120に渡す。通信制御手段2120は、該ユーザデータと通信端末220のアドレスBとの組を暗号装置410に送る。

【0021】該ユーザデータと通信端末220のアドレスBとの組は、ユーザデータ送受信手段4140に渡される。ユーザデータ送受信手段4140は、該ユーザデータと通信端末220のアドレスBとの組をユーザデータ暗号化/復号手段4130に渡す。ユーザデータ暗号化/復号手段4130は、通信端末220のアドレスBにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、通信相手アドレスBとの組として記憶されているセッション鍵を用いて、該ユーザデータを暗号化する。これを暗号化ユーザデータとし、該暗号化

ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段4140に渡す。ユーザデータ送受信手段4140は、該暗号化ユーザデータと通信相手アドレスBとの組より、暗号化ユーザデータの情報を含むユーザデータ送信コマンドを暗号装置420に送る。

【0022】暗号装置420により受信されたユーザデータ送信コマンドは、ユーザデータ送受信手段4240に渡される。ユーザデータ送受信手段4240は、該ユーザデータ送信コマンドに含まれる暗号化ユーザデータ及び通信相手アドレスAの情報を求め、該暗号化ユーザデータとアドレスAの組をユーザデータ暗号化/復号手段4230に渡す。ユーザデータ暗号化/復号手段4230は、通信相手アドレスAにより、記憶装置に記憶されているアドレスとセッション鍵の組を照合し、アドレスAとの組として記憶されているセッション鍵を用いて、該ユーザデータを復号する。これをユーザデータとし、該ユーザデータと通信相手アドレスとの組をユーザデータ送受信手段4240に渡す。ユーザデータ送受信手段4240は、該ユーザデータとアドレスとの組を通信端末220に渡す。通信端末220に渡された該ユーザデータと通信相手アドレスとの組は、通信制御手段2220に渡される。通信制御手段2220は、該ユーザデータと通信相手アドレスとの組をアプリケーション2210に渡す。

【0023】以上のように、従来の暗号通信システムにおいては、任意の通信相手との実際のユーザデータの送受信の手順を行う際には、その手順を行うたび毎に、これに先立って鍵配送の手順を行う必要がある。また、通信相手毎に暗号鍵の情報を登録する必要がある。また、暗号を用いるために、通信端末に暗号通信制御手段という特別の手段を追加する必要がある。

【0024】また、特開昭54-93937号には、複数ドメイン・データ通信ネットワークにおける“暗号装置用共通操作キー設定装置”について開示されている。

【0025】

【発明が解決しようとする課題】以上述べたように、従来の暗号データ通信の手順によれば、通信端末は各通信相手毎に通信を開始するに先立ち、その通信で用いるセッション鍵を鍵管理装置に要求し、それに応じて鍵管理装置から通信端末にセッション鍵を配達するようになっていた。そのため、同じ部所の通信端末同志をグループ化することに関しては、考慮されていなかった。また、暗号装置に接続された通信端末は、電子メール等の平文(暗号化されない文)を送受信することができないという課題があった。また、通信相手となる通信端末、アプリケーション、通信方向により平文通信とするか暗号通信とするか、設定することはできなかった。また、複数の鍵の中から任意の鍵を用いて暗号化するという設定もできなかった。また、1台の暗号装置に複数台の通信端末が接続される場合、通信端末毎に異なる条件で暗号化

することはできなかった。また、特開昭 54-93937 号では、複数ドメイン間でデータ通信を暗号化するための共通の暗号化鍵を設定することが述べられていたが、共通の暗号化鍵を用い複数の重複したグループを実現する方式は、述べられていなかった。

【0026】本発明は、上記のような課題を解決するためになされたもので、1つのネットワーク上の暗号データ通信を行う通信装置から、複数の物理グループを形成できる暗号化システムを提供することを目的とする。また、任意の暗号装置において、暗号通信と平文通信を切り換えることができる暗号化システムを提供することを目的とする。また、同一のネットワーク上、あるいは、複数ドメイン間で複数の重複した論理グループを実現する暗号化システムを提供することを目的とする。

【0027】

【課題を解決するための手段】この発明に係る暗号化システムは、グループ化された複数の通信装置と、少なくとも上記複数の通信装置の1つ以上の通信装置に対応してそれぞれ設けられた複数の暗号装置であって、上記グループに属する通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段とを備えた複数の暗号装置とを備えたことを特徴とする。

【0028】上記暗号装置は、上記セッション鍵記憶手段にセッション鍵を少なくとも1つ記憶し、上記セッション鍵により通信データを暗号化あるいは復号するか否か設定するモードスイッチを備えることを特徴とする。

【0029】上記暗号装置は、更に、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備えることを特徴とする。

【0030】上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする。

【0031】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【0032】上記暗号化条件は、通信方向により定まることを特徴とする。

【0033】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定め、上記条件判定手段は、上記暗号化条件からいずれのセッション鍵を用いて暗号化あるいは復号するか判定することを特徴とする。

【0034】上記暗号化システムは、更に、グループ化された通信装置を記憶する通信装置グループ記憶手段

と、上記通信装置グループ記憶手段により記憶されたグループ毎に個別のセッション鍵を生成して出力するセッション鍵生成手段とを備えた鍵管理装置を備えることを特徴とする。

【0035】上記鍵管理装置は、更に、上記暗号装置に備えられた上記モードスイッチの切り替えを有効とするか無効とするかを示す有効無効情報を暗号装置毎に設定し、有効無効情報を対応する暗号装置に送信する有効無効設定手段を備え、上記暗号装置は、更に、上記モードスイッチの設定と送信された上記有効無効情報とから通信データを暗号化あるいは復号するか判定する有効無効判定手段を備えることを特徴とする。

【0036】上記鍵管理装置は、上記暗号化条件を設定し、上記暗号化条件を上記暗号装置に送信して暗号化条件記憶手段に記憶させる暗号化条件設定手段を備えることを特徴とする。

【0037】上記鍵管理装置は、更に、上記セッション鍵生成手段により生成されたセッション鍵を暗号化するセッション鍵暗号化手段と、上記暗号化されたセッション鍵を上記通信装置グループ記憶手段により記憶されたグループに対応付けられた暗号装置に送信するセッション鍵送信手段と、上記暗号装置は、更に、鍵管理装置のセッション鍵送信手段により送信された暗号化されたセッション鍵を受信するセッション鍵受信手段と、上記暗号化されたセッション鍵を復号するセッション鍵復号手段とを備えることを特徴とする。

【0038】この発明に係る暗号化システムは、複数の鍵管理装置を備え、各鍵管理装置と1以上の暗号装置と1以上の通信装置とからなる暗号管理ドメインを形成する暗号化システムにおいて、上記複数の鍵管理装置は、それぞれの暗号管理ドメインで用いるセッション鍵を生成するセッション鍵生成手段を備え、上記複数の鍵管理装置の中の1台の鍵管理装置におけるセッション鍵生成手段は、更に、複数の暗号管理ドメイン同士の暗号通信において用いられる共通セッション鍵を他の鍵管理装置のために生成することを特徴とする。

【0039】上記暗号装置は、通信装置が送受信する通信データを暗号化あるいは復号するセッション鍵を少なくとも1つ記憶するセッション鍵記憶手段と、上記セッション鍵により通信データを暗号化あるいは復号する暗号処理手段と、上記暗号処理手段により処理された通信データを送受信するデータ送受信手段と、通信データの暗号化に関する暗号化条件を記憶する暗号化条件記憶手段と、上記暗号化条件に基づいて通信データを暗号化あるいは復号するか否か判定する条件判定手段とを備え、上記鍵管理装置は、更に、上記セッション鍵生成手段が生成した複数のセッション鍵を記憶するセッション鍵テーブルと、上記暗号化条件を暗号装置に送信して上記暗号化条件記憶手段に記憶させる暗号化条件設定手段とを備えることを特徴とする。

【0040】上記暗号化条件は、特定の通信に関する暗号化条件を設定した1以上の特例バスと上記特例バスに合致しない全ての通信に対する暗号化条件を設定した基本バスとからなることを特徴とする。

【0041】上記暗号化条件は、通信データを用いるアプリケーションプログラムにより定まることを特徴とする。

【0042】上記暗号化条件は、通信方向により定まることを特徴とする。

【0043】上記暗号装置は、上記セッション鍵記憶手段に複数のセッション鍵を記憶し、上記暗号化条件は、いずれのセッション鍵を用いて暗号化するか定めることを特徴とする。

【0044】上記暗号化条件は、通信相手となる1以上の通信装置により定まることを特徴とする。

【0045】上記暗号装置は、通信装置あるいは鍵管理装置を接続する1以上のポートを備え、ポート毎に上記基本バスと上記特例バスをポート条件として記憶するポート条件記憶手段を備えることを特徴とする。

【0046】上記鍵管理装置が上記ポート条件を生成し、各暗号装置のポート条件記憶手段に配布することを特徴とする。

【0047】

【発明の実施の形態】

実施の形態1. この実施の形態では、各暗号装置にセッション鍵を1つ記憶し、暗号通信と平文通信（暗号化しない通信）を切り換えることのできる暗号化システムについて述べる。

【0048】図1は、この実施の形態におけるネットワークシステムの一例を示す図である。2本のLAN (Local Area Network) がルータ/ブリッジ12によりLAN/WAN (Wide Area Network) 15と接続されているネットワークシステムである。LAN1には、鍵管理装置3が暗号装置49を介して接続される。更に、LAN1には、暗号装置41, 42, 43を介し、通信端末（通信装置とも言う）21, 22, 23が接続される。また、暗号装置を介さない通信端末24, 25が接続される。更に、ネットワーク管理装置13が接続される。図では、鍵管理装置3に暗号装置49が接続されているが、これは鍵管理装置3が他の通信端末と共にグループを構成する場合を想定している。そのため、鍵管理装置3に暗号装置49が接続されなくともよい。また、1台の暗号装置に対し、複数台の通信端末を接続してもよい。

【0049】暗号装置41～43は、LAN1と通信端末21～23との間に置かれ、通信データのデータ部を暗号化/復号することで、LAN1上を流れる通信データの盗聴を防止する。ユーザデータの暗号化は、高速で秘匿性の高い独自の秘密鍵暗号方式による。暗号範囲は、暗号装置を出てネットワーク上を通り、通信先の暗

号装置へ入るまでである。鍵管理装置3は、暗号装置に対するデータを暗号化するセッション鍵を配信するとともに、暗号装置41～43の状態を常時監視する。

【0050】図2は、この実施の形態における暗号化システムのブロック図である。図2において、LAN1に鍵管理装置3と暗号装置41, 42, 43が接続されている。鍵管理装置3には、入出力装置5が接続される。暗号装置41, 42, 43には、通信端末21, 22, 23が接続される。図には、暗号装置41, 42及び通信端末21, 22が図示されているが、通常は更に多くの暗号装置及び通信端末が接続される。また、説明を簡単にするために、鍵管理装置3には、暗号装置が接続されない例を示してある。また、1台の暗号装置に対し、1台の通信端末が接続される例を図示してある。通信端末21, 22は、それぞれアプリケーション211, 221、通信制御手段212, 222から構成される。鍵管理装置3は、セッション鍵生成手段3-1、セッション鍵管理手段3-2、セッション鍵送信開始検出手段3-3、セッション鍵暗号化手段3-4、セッション鍵送信手段3-5、通信装置グループ記憶手段3-7、有効無効設定手段6-1からなる。セッション鍵生成手段3-1は、データを暗号化するセッション鍵を生成する。セッション鍵暗号化手段3-4は、セッション鍵生成手段3-1により生成されたセッション鍵を、鍵暗号化鍵を用いて暗号化する。セッション鍵送信手段3-5は、セッション鍵を各暗号装置に送信する。通信装置グループ記憶手段3-7は、グループ化された通信装置を記憶する。有効無効設定手段6-1は、暗号装置に備えられたモードスイッチの切り換えを有効とするか無効とするかを示す有効無効情報を、暗号装置毎に設定する。そして、設定した有効無効情報を対応する暗号装置に送信する。

【0051】暗号装置41, 42は、セッション鍵復号手段411, 421、セッション鍵受信手段412, 422、暗号処理手段413, 423、データ送受信手段414, 424、セッション鍵記憶手段711, 721、モードスイッチ712, 722、有効無効判定手段713, 723からなる。セッション鍵受信手段412, 422は、鍵管理装置3から送信された暗号化されたセッション鍵を受信する。セッション鍵復号手段411, 421は、セッション鍵受信手段412, 422により受信された暗号化されたセッション鍵を、それぞれの暗号装置独自の鍵暗号化鍵により復号する。暗号処理手段413, 423は、セッション鍵により通信データを暗号化、あるいは、復号する。データ送受信手段414, 424は、暗号処理手段413, 423により処理された通信データを送受信する。セッション鍵記憶手段711, 721は、通信データを暗号化、あるいは、復号するセッション鍵を少なくとも1つ記憶する。モードスイッチ712, 722は、この暗号装置における通信データを、暗号通信とするか平文通信とするかを設定す

るスイッチである。有効無効判定手段 713, 723 は、暗号装置におけるモードスイッチ 712, 722 の設定と、鍵管理装置 3 から送信された有効無効情報とから通信データを暗号通信とするか平文通信とするかを判定する。

【0052】セッション鍵と鍵暗号化鍵について述べる。セッション鍵は、ユーザデータを暗号化する鍵である。これに対し、鍵暗号化鍵は、セッション鍵を暗号化する鍵である。鍵暗号化鍵は、鍵管理装置 3 から各暗号装置にセッション鍵を配送する際、第三者にセッション鍵を知られることなく配送するために用いる。鍵管理装置 3 のセッション鍵暗号化手段 34 で、セッション鍵を鍵暗号化鍵で暗号化する。暗号装置 41, 42 のセッション鍵復号手段 411, 421 で、配送された暗号化されたセッション鍵を、鍵暗号化鍵で復号する。鍵暗号化鍵は、暗号装置毎に異なる。鍵暗号化鍵の設定方法は、通信回線を介さない。

【0053】次に、鍵暗号化鍵の設定手順を述べる。

1. 鍵管理装置 3 で、各暗号装置毎に異なる鍵暗号化鍵を作成する。
2. 暗号装置に接続したローカルコンソールより鍵暗号化鍵を設定するコマンドを入力し、鍵入力モードにする。
3. 鍵管理装置で作成した鍵暗号化鍵を、暗号装置のローカルコンソールより入力する。
4. 暗号装置を立ち上げ直す。

【0054】セッション鍵は、ユーザデータを暗号化／復号するために使用する。同一グループの暗号装置のセッション鍵は、全て同じである。但し、後述の実施の形態で述べるように、セッション鍵を複数用意すれば、暗号装置間で重複した論理グループを作ることが可能である。セッション鍵の設定方法は、オンラインで設定する。

【0055】次に、セッション鍵を暗号装置の要求に応じ、設定する手順の概略を述べる。

1. 鍵管理装置 3 で、セッション鍵を作成する。
2. 作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。
3. 暗号装置の電源を入れることにより、自動的に暗号装置からセッション鍵を送信してもらうよう要求コマンドが、鍵管理装置 3 へ送られる。
4. 鍵管理装置 3 から暗号化されたセッション鍵が要求のあった暗号装置へ送られる。

【0056】次に、他の方法として、セッションの鍵を管理者の指示により、設定する手順の概略を述べる。

1. 鍵管理装置 3 で、セッション鍵を作成する。
2. 作成したセッション鍵を、各暗号化装置毎に異なる鍵暗号化鍵で暗号化する。
3. 管理者の指示により、新しいセッション鍵を送信する暗号装置の範囲を決定する。範囲の種類は、大きく分

けて、以下の 4 種類がある。

- (1) 直前の暗号装置の状態確認の時に、電源が ON であった暗号装置全て。
- (2) 直前の暗号装置の状態確認の時に、電源が ON で、かつ、予め指定されたグループ内の暗号装置全て。
- (3) 指定された暗号装置。
- (4) 全ての暗号装置。

4. 決定された範囲に含まれる暗号装置全てに、暗号化されたセッション鍵を配信する。

【0057】更に、他の方法として、鍵管理装置 3 にタイマを備え、一定時間が経過すると自動的にセッション鍵を生成し、同一グループに属する暗号装置に配信する手順を図 2 を用いて詳しく述べる。LAN 1 に接続された同一グループに属する各暗号装置に対し、一定時間毎にセッション鍵を鍵管理装置 3 から配布し、それまで設定されていたセッション鍵を直ちに配布されたセッション鍵で置き換える例である。通信端末 2-1 と通信端末 2-2、即ち、暗号装置 41, 42 がグループ A としてグループ化され、通信装置グループ記憶手段 37 に登録されている。グループ A 対応のタイマは、鍵管理装置 3 のセッション鍵送信開始検出手段 33 に存在している。暗号通信を行う際には、鍵配信の手順と実際のユーザデータの送受信の手順が必要であるが、鍵配信の手順と実際のユーザデータの送受信の手順は、独立に行なうことが特徴である。

【0058】図 3 は、セッション鍵の配信の手順を示すシーケンス図である。S1 はセッション鍵配信コマンド KEYDIST、S2 はセッション鍵受信確認コマンド KEYDIST_ACK、S3 はセッション鍵配信コマンド KEYDIST、S4 はセッション鍵受信確認コマンド KEYDIST_ACK である。

【0059】(手順 1-1) 鍵管理装置 3 のセッション鍵送信開始検出手段 33 のグループ A 対応のタイマがタイムアウトすると、セッション鍵送信開始検出手段 33 がセッション鍵送信開始検出信号をセッション鍵管理手段 32 に渡す。

(手順 1-2) セッション鍵管理手段 32 は、該セッション鍵送信開始検出信号を受け取ると、セッション鍵生成手段 31 を起動する。

【0060】(手順 1-3) セッション鍵生成手段 31 は、セッション鍵管理手段 32 により起動されると乱数を発生し、これをセッション鍵としてセッション鍵管理手段 32 に渡す。

(手順 1-4) セッション鍵管理手段 32 は、該セッション鍵をグループ A のセッション鍵として記憶装置に記憶する。セッション鍵管理手段 32 は、通信装置グループ記憶手段 37 からグループ A に属する暗号装置を検索し、暗号装置 41 を選ぶ。セッション鍵管理手段 32 は、セッション鍵暗号化手段 34 に該セッション鍵を渡し、暗号装置 41 に対する鍵暗号化である旨を知らせ

る。

(手順1-5) セッション鍵暗号化手段34は、該セッション鍵を暗号装置41に対応する鍵暗号化鍵により暗号化し、その結果を暗号化セッション鍵としてセッション鍵管理手段32に渡す。

【0061】(手順1-6) セッション鍵管理手段32は、該暗号化セッション鍵と、暗号装置41のアドレスをセッション鍵送信手段35に渡す。

(手順1-7) セッション鍵送信手段35は、該暗号化セッション鍵の情報を含んだセッション鍵配信コマンドKEYDISTを生成し、これを記憶装置に記憶する。セッション鍵送信手段35は、該セッション鍵配信コマンドKEYDISTを、渡されたアドレスにより暗号装置41に対して送信する(S1)。

(手順1-8) 暗号装置41のセッション鍵受信手段412により、該セッション鍵配信コマンドKEYDISTは受信される。

(手順1-9) セッション鍵受信手段412は、該セッション鍵配信コマンドKEYDISTから暗号化セッション鍵を含むデータ部分を抽出し、セッション鍵復号手段411に渡す。

(手順1-10) セッション鍵復号手段411は、該暗号化セッション鍵を含むデータ部分を、予め別の手段により設定されている暗号装置41独自の鍵暗号化鍵により復号する。そして、その結果をセッション鍵としてセッション鍵受信手段412に渡す。

【0062】(手順1-11) セッション鍵受信手段412は、鍵管理装置3に対しセッション鍵受信確認コマンドKEYDIST_ACKを送信する(S2)。更に、該セッション鍵をセッション鍵記憶手段711に記憶する。

(手順1-12) 鍵管理装置3により受信された暗号装置41からのセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段35に渡される。セッション鍵送信手段35は、セッション鍵管理手段32に対し、暗号装置41へセッション鍵配信完了を通知する。セッション鍵管理手段32は、セッション鍵暗号化手段34にグループAのセッション鍵を渡し、暗号装置42に対する暗号化である旨を知らせる。

(手順1-13) セッション鍵暗号化手段34は、上記(手順1-5)と同様にして、暗号装置42に対応する暗号化セッション鍵を作成する。セッション鍵送信手段35は、該暗号化セッション鍵の情報を含んだセッション鍵配信コマンドKEYDISTを作成し、暗号装置42に送信する(S3)。

(手順1-14) 暗号装置42のセッション鍵受信手段422により、該セッション鍵配信コマンドは受信される。

(手順1-15) セッション鍵受信手段422は、該セッション鍵配信コマンドから暗号化セッション鍵を抽出

し、該暗号化セッション鍵をセッション鍵復号手段421に渡す。

【0063】(手順1-16) セッション鍵復号手段421は、該暗号化セッション鍵を予め別の手段により設定されている独自の鍵暗号化鍵により復号する。その結果をセッション鍵として、セッション鍵受信手段422に渡す。

(手順1-17) セッション鍵受信手段422は、鍵管理装置3に対しセッション鍵受信確認コマンドKEYDIST_ACKを送信する(S4)。更に、該セッション鍵をセッション鍵記憶手段721に記憶する。

(手順1-18) 鍵管理装置3により、受信されたセッション鍵受信確認コマンドKEYDIST_ACKは、セッション鍵送信手段35に渡される。

(手順1-19) セッション鍵送信手段35は、暗号装置42へのセッション鍵配信完了をセッション鍵管理手段32に通知する。セッション鍵管理手段32は、グループAに属する他の暗号装置がないことから、グループAに対する鍵配信は、完了したと判断する。

【0064】以上の手順に従って、鍵配信が行われることにより、同一グループに属する暗号装置41と暗号装置42が共通のセッション鍵を持つことができる。この後、通信端末21のアプリケーション211が、LAN1を介して接続されている通信端末22のアプリケーション221と通信を行う。アプリケーション211のユーザデータは、暗号装置41の暗号処理手段413で暗号化され、暗号装置42の暗号処理手段423で復号され、アプリケーション221に渡される。

【0065】また、上記のセッション鍵送信開始検出手段33におけるセッション鍵送信開始検出信号をタイマによらず、鍵管理装置3の管理者による手動の入力操作により、出力するようにしてもよい。また、上記のセッション鍵送信開始検出手段33におけるセッション鍵送信開始検出信号を、暗号装置の立ち上げ状態を検出することにより出力するようにしてもよい。

【0066】なお、上記2台の暗号装置へ鍵配信を行う手順を示したが、同一のグループに属する任意の台数の暗号装置に対しても、同様に行うことができる。セッション鍵の変更を、セッション鍵の配信／受信と同時に進行例を示した。しかし、通信を一度停止してからセッション鍵を新しい鍵に変更してもよいし、セッション鍵の配信／受信から所定時間経過後に変更してもよい。

【0067】次に、本実施の形態の要点である暗号通信と平文通信の切り換えについて述べる。図4は、暗号化システムにおけるグループ分けを説明するための図である。鍵管理装置3は、暗号装置49を介し、LAN1に接続される。通信端末20～22、25～29は、暗号装置41～46を介し、LAN1に接続される。通信端末21と22は、同一の暗号装置42に接続される。通信端末28と29は、同一の暗号装置46に接続され

る。更に、通信装置 23, 24 が暗号装置を介さず、LAN 1 に接続されている。鍵管理装置 3 と暗号装置 4 9 は、グループ A とする。暗号装置 4 1 ~ 4 3 と通信端末 2-0 ~ 2-2, 2-5 は、グループ B とする。暗号装置 4 4 ~ 4 6 と通信端末 2 6 ~ 2 9 は、グループ C とする。これらのグループは、通信装置グループ記憶手段 3 7 により記憶される。ここで、例えば、通信端末 2 0 から送信されたユーザデータは、暗号装置 4 1 で暗号化される。暗号化されたデータを受信できる可能性のある通信端末は、通信端末 2 1, 2 2, 2 5 である。暗号装置を介さない通信端末 2 3, 2 4 とグループ C に属する通信端末 2 6 ~ 2 9 は、通信データを復号できないため、受信することができない。このように、暗号通信において、同一暗号グループの暗号装置に接続されている通信端末間は、あたかも平文通信のように通信できる。しかし、暗号グループが異なる又は暗号装置が接続されていない通信端末では、暗号化された通信文を受信しても復号できないため盗聴できない。もし、暗号装置そのものを盗まれても、どの暗号グループに属しているかは、暗号装置側からは見分けられないので、なりすましも防げる。

【0068】ところが、暗号グループが異なる又は暗号装置が接続されていない通信端末と通信したい場合は、暗号装置から出入りする通信を、暗号化/復号することを止めなければならない。この切り換えを暗号装置 4 1, 4 2, ..., が持っているモードスイッチ 7 1 2, 7 2 2, ... の ON/OFF で実現する。モードスイッチ 7 1 2, 7 2 2, ... を ON すると、平文通信となり、OFF にすると、暗号通信となる。しかし、暗号装置は、通信端末利用者が勝手に操作できるため、モードスイッチの ON/OFF のみで暗号通信を平文通信に変更できるのは、セキュリティ上好ましくない。そこで、鍵管理装置でモードスイッチの切り換えを有効とするか無効とするか、暗号装置毎に有効無効情報を設定する。これにより、鍵管理装置で平文通信と暗号通信の切り換えができる暗号装置を管理することができる。

【0069】図 5 は、鍵管理装置 3 で設定された有効無効情報と有効無効情報を入力する画面である。この画面の表示及び以下に述べるオペレーションは有効無効設定手段 6 1 により実行される。新たにデータを入力する場合は、入力フィールドから入力する。入力フィールドから入力するデータとして、グループナンバ (GN)、IP アドレス、備考、有効/無効情報がある。画面に表示されるグループ名称は、グループナンバ (GN) が入力されると自動的に画面に出力される。有効無効情報は、予め '0' (無効) がセットされている。有効としたい場合は、'1' を入力する。表示されているデータは、上から順に図 4 で示した暗号装置 4 9, 4 1 ~ 4 6 に対応する。暗号装置 4 1 と 4 6 の有効無効情報が有効とされている。ここで、有効とは、該暗号装置のモードスイッチの切り換えが有効という意味である。無効とは、暗

号装置でモードスイッチが切り換えられても、無効とするという意味である。

【0070】鍵管理装置 3 が暗号化されたセッション鍵を、各暗号装置へ KEYDIST コマンドにより配達する際、有効無効情報も付加して送る。図 6 に、KEYDIST コマンドの内容を示す。図 6 において、プロトコルタイプは、通信プロトコルのタイプを示す。認証用データは、配達された暗号装置で復号できたか否かチェックするための固定パターンである。暗号装置で復号されたデータの一部が固定パターンと一致すれば、復号が正しく行われたことを示す。最後のビットに、有効無効情報がセットされる。'1' は有効を示し、'0' は無効を示す。以上のように、KEYDIST コマンドの内容の内、データが設定されない部分は、0 とする。そして、セッション鍵及び有効無効情報などが設定された KEYDIST コマンドの内容は、鍵暗号化鍵で暗号化され送信される。

【0071】鍵管理装置 3 における有効無効設定手段 6 1 は、入力画面により設定された有効無効情報を、セッション鍵配達コマンド KEYDIST を生成するセッション鍵送信手段 3 5 に渡す。セッション鍵送信手段 3 5 は、図 6 で示したように、最後のビットに有効無効情報をセットした KEYDIST コマンドを生成する。次に、暗号装置 4 1 を例に取ると、セッション鍵受信手段 4 1 2 が KEYDIST コマンドを受信し、セッション鍵復号手段 4 1 1 に渡す。セッション鍵復号手段 4 1 1 が復号し、復号したセッション鍵をセッション鍵受信手段 4 1 2 に渡す。セッション鍵受信手段 4 1 2 は、復号された KEYDIST の内容から有効無効情報を取り出し、有効無効判定手段 7 1 3 に渡す。有効無効判定手段 7 1 3 は、モードスイッチ 7 1 2 のスイッチの ON/OFF と、有効無効情報の論理積によって暗号通信とするか平文通信とするか判定する。

【0072】図 7 に、モードスイッチの情報と有効無効情報の論理積を表として示す。モードスイッチ OFF は (0) であり、ON は (1) である。有効無効情報が、有効は (1) であり、無効は (0) である。そのため、論理積を取ると、モードスイッチ ON であり、かつ、有効無効情報が有効の場合のみ (1)、即ち、ユーザデータは透過となる。それ以外の場合は、全てモードスイッチの設定如何に関わらず、暗号化される。なお、透過とは、平文通信とすることである。

【0073】図 8 は、図 4 のように、グループ化された暗号化システムにおいて、平文通信を採用する場合である。暗号装置 4 1, 4 3, 4 4, 4 6 のモードスイッチが ON となっている。即ち、これらの暗号装置は、平文通信とするようモードスイッチが切り換えられている。ところが鍵管理装置 3 の有効無効情報は、図 5 で示したように、暗号装置 4 1 と 4 6 のみ有効となっている。そのため、通信端末 2 0 から送られたユーザデータは、暗

号装置 4 1 では暗号化されず、平文で送信される。平文通信であるため、暗号装置のない通信端末 2 3, 2 4 で受け取ることができる。また、暗号装置 4 6 のモードスイッチが ON であり、有効無効情報が有効であるため、通信端末 2 0 からの通信データを復号しない。そのため、通信端末 2 8, 2 9 は、通信端末 2 0 の送出した平文通信を受け取ることができる。暗号装置 4 3, 4 4 は、モードスイッチが ON ではあるが、有効無効情報が無効となっているため、平文通信を受け取ることができない。また、暗号装置 4 1 は、グループ B に属するが、暗号装置 4 6 は、グループ C に属する。平文通信することにより、暗号装置のない通信端末、あるいは、異なるグループの通信端末とでも通信することができる。

【0074】以上のように、この実施の形態の暗号化システムは、暗号装置のセッション鍵をグループ単位で同じものとすることにより、異なるグループ間の通信を禁止することができる。また、ネットワーク上での盗聴を防止することができる。更に、暗号通信とするか平文通信とするか、暗号装置側及び鍵管理装置の設定で選択することができ、異なるグループの通信端末、あるいは、暗号装置を持たない通信端末と通信することもでき、より柔軟な暗号化システムを形成することができる。更に、暗号装置のモードスイッチにより、暗号通信とするか平文通信とするか設定し、加えて鍵管理装置で暗号装置のモードスイッチが有効であるか無効であるか一括管理することができるため、より確実なセキュリティ管理が行える。

【0075】また、図 2 の暗号装置のブロック図において、暗号装置 4 1, 4 2 のモードスイッチ 7 1 2, 7 2 2 を取り去ってもよい。この場合、鍵管理装置 3 の有効無効設定手段 6 1 で、有効と設定した暗号装置を平文通信とすると決めてよい。有効無効設定手段 6 1 で無効と設定した暗号装置は、暗号通信を行う。有効無効設定手段 6 1 で設定した有効無効情報は、鍵管理装置 3 から暗号装置 4 1, 4 2 の有効無効判定手段 7 1 3, 7 2 3 に送信され、各暗号装置の有効無効判定手段が暗号通信とするか平文通信とするか判定する。

【0076】また、図 2 の暗号化システムのブロック図において、鍵管理装置 3 の有効無効設定手段 6 1 と、暗号装置 4 1, 4 2 の有効無効判定手段 7 1 3, 7 2 3 を省いてもよい。この場合、暗号装置 4 1, 4 2 のモードスイッチ 7 1 2, 7 2 2 の ON / OFF により、暗号通信とするか平文通信とするか設定する。

【0077】また、図 9 に、鍵管理装置 3 a がセッション鍵を配達しない場合のブロック図を示す。図 9 に示すように、鍵管理装置 3 a は、図 2 で示したセッション鍵送信開始検出手段 3 3, セッション鍵暗号化手段 3 4, セッション鍵送信手段 3 5 を省く。暗号装置 4 1 a, 4 2 a は、セッション鍵復号手段 4 1 1, 4 2 1, セッション鍵受信手段 4 1 2, 4 2 2 を省く。この場合、鍵管

理装置 3 a において、通信装置グループ記憶手段 3 7 に記憶されたグループ毎に、セッション鍵をセッション鍵生成手段 3 1 により生成する。鍵管理装置 3 a で生成されたセッション鍵は、ネットワークを用いた通信によらず、各暗号装置のセッション鍵記憶手段に記憶する。他の働きは、上述の説明と同様である。

【0078】図 10 に、図 2 で示した暗号化システムの鍵管理装置がない場合を示す。LAN 1 に暗号装置 4 1 b, 4 2 b を介し、通信端末 2 1, 2 2 が接続される。暗号装置及び通信端末は、図示していないが、他にも接続されている。暗号装置 4 1 b, 4 2 b は、セッション鍵記憶手段 7 1 1, 7 2 1, 暗号処理手段 4 1 3, 4 2 3, データ送受信手段 4 1 4, 4 2 4, モードスイッチ 7 1 2, 7 2 2 からなる。通信端末 2 1, 2 2 は、図 2 と同様である。セッション鍵は、セッション鍵生成手段と同様の働きを有する図示していない処理装置において作成され、それぞれ暗号装置 4 1 b, 4 2 b のセッション鍵記憶手段 7 1 1, 7 2 1 に入力され、記憶される。セッション鍵の同じ暗号装置同志が同一グループとなる。モードスイッチ 7 1 2, 7 2 2 のスイッチの ON / OFF により、暗号通信とするか平文通信とするか決まる。

【0079】実施の形態 2. この実施の形態は、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか、暗号化条件を設定することができる暗号化システムについて述べる。更に、複数のセッション鍵を 1 台の暗号装置に保有し、通信相手、アプリケーション、通信方向によりどのセッション鍵を用いるか、暗号化条件を設定することができる暗号化システムについて述べる。

【0080】図 11 は、この実施の形態における暗号化システムのブロック図である。LAN 1 に鍵管理装置 6 と暗号装置 8 1, 8 2 が接続されている。鍵管理装置 6 には、入出力装置 5 が接続されている。暗号装置 8 1, 8 2 には、通信端末 2 1, 2 2 が接続されている。鍵管理装置 6 は、セッション鍵生成手段 3 1, セッション鍵管理手段 3 2, セッション鍵送信開始検出手段 3 3, セッション鍵暗号化手段 3 4, セッション鍵送信手段 3 5, 通信装置グループ記憶手段 3 7, 暗号化条件設定手段 6 2 からなる。暗号装置 8 1 は、セッション鍵復号手段 4 1 1, セッション鍵受信手段 4 1 2, 暗号処理手段 4 1 3, データ送受信手段 4 1 4, セッション鍵記憶手段 7 1 1, 暗号化条件記憶手段 8 1 1, 条件判定手段 8 1 2 からなる。暗号装置 8 2 も同様の構成である。通信端末 2 1, 2 2 は、図 2 と同様である。暗号装置の暗号化条件記憶手段 8 1 1, 8 2 1 は、通信データの暗号化に関する暗号化条件を記憶する。暗号化条件としては、通信相手となる通信装置、アプリケーション、通信方向により暗号通信とするか平文通信とするか設定する。更に、複数のセッション鍵を暗号装置に保有し、通信相

手、アプリケーション、通信方向によりどのセッション鍵を用いるか暗号化条件で設定する。暗号化条件記憶手段811, 821は、これらの暗号化条件を記憶する。暗号化条件を設定するのは、鍵管理装置6の暗号化条件設定手段62により鍵管理装置6の管理者が、それぞれの暗号装置に関し条件を設定し、各暗号装置に送信する。あるいは、鍵管理装置6の暗号化条件設定手段62は省き、それぞれの暗号装置における暗号化条件記憶手段811, 821において、それぞれの暗号装置の使用者が暗号化条件を、暗号化条件記憶手段811, 821に設定してもよい。条件判定手段812, 822は、暗号化条件記憶手段811, 821に記憶された暗号化条件と受信した通信データの通信相手となる通信装置、通信方向、アプリケーション、更に複数のセッション鍵がある場合には、セッション鍵により平文通信とするか暗号通信とするか、あるいは、いずれのセッション鍵を用いるか判定する。

【0081】図12は、この実施の形態における暗号化システムを利用したネットワークシステムの例である。サーバ91、WWW (World Wide Web) 代理サーバ92、メールサーバ94がルータ14を介してインターネット16につながっている。また、WWW93がインターネット16に接続されている。暗号装置81, 82が、LAN1に接続されている。暗号装置81は、通信端末21, 22を接続する。暗号装置82は、通信端末23, 24を接続する。LAN1には、この他にも暗号装置及び通信端末が接続されているが、図では省く。暗号装置81, 82は、グループAに属する。

【0082】図12のネットワーク例において、暗号装置81の暗号化条件を次のように設定する。

基本バス：アプリケーション（全）、暗号

特例1：IPアドレス（メールサーバ）&アプリケーション（メール）&通信方向（出）、透過

特例2：IPアドレス（WWW代理サーバ）&アプリケーション（http）&通信方向（出）、透過

特例3：IPアドレス（サーバ）&アプリケーション（ネームサーバ）、透過

【0083】上記の暗号化条件は、基本バスと特例バスがあるが、特例バスで示した条件の方が優先順位は高い。通常の通信は、基本バスで指定された暗号化条件に従う。しかし、特例1, 2, 3で指定された暗号化条件に適合する通信データの場合、特例バスで示された条件を優先する。図12を用いて説明すると、通信端末21、あるいは、22からグループA内の通信端末23、あるいは、24へ通信を送る場合は、基本バスの暗号化条件に従い、全てのアプリケーションの通信データについて暗号化する。この通信の流れを図では、点線で示す。通信端末21, 22からメールサーバ94へメールを送る場合、特例1の暗号化条件に適合し透過、即ち、

平文通信となる。通信端末21, 22からWWW代理サーバ92にアプリケーション（http）のユーザデータを送信する場合、特例2に適合し平文通信となる。通信端末21, 22からサーバ91へアプリケーション（ネームサーバ）で通信データを送受信する場合、特例3に従い平文通信となる。特例3では、通信方向を指定していないので、送受信する両方向のデータについて透過、即ち、平文通信となる。なお、暗号装置82の暗号化条件は、暗号装置81と異なってもよい。また、暗号装置に複数の通信端末が接続されている場合は、接続された端末毎に異なる暗号化条件（特例バス）を設定してもよい。なお、基本バス、特例バスについては、後述の実施の形態で更に詳しく説明する。このように、1台の暗号装置でグループ内の通信は暗号化し、公共的なメールサービスやWWWサービスを平文で受けることができる。

【0084】図13は、この実施の形態における暗号化システムの他のネットワーク例である。インターネット16に、WWWサーバ95とメールサーバA96が接続されている。ルータ14を介し、2本のLAN1が接続され、一方のLAN1に暗号装置81が接続される。暗号装置81には、通信端末21と社内メールサーバ97が接続される。また、もう一方のLAN1には暗号装置82が接続される。暗号装置82には、社内メールサーバ98と通信端末22が接続される。暗号装置81と82及び通信端末21, 22、社内メールサーバ97, 98は、同一のグループに属する。

【0085】図13のネットワーク例において、暗号装置81の暗号化条件を次のように設定する。

基本バス：アプリケーション（メール+WWW）、透過
特例1：IPアドレス（全ての社内の暗号装置のアドレス）&アプリケーション（全）、暗号

【0086】上記のように、暗号化条件を設定すると、暗号装置81を通過する全ての社内メールや社内のアプリケーション・データは暗号化され、インターネット16に接続された公共のメールサーバA96のメールや、WWWサーバ95との通信データのやりとりは透過、即ち、平文通信となる。このように、インターネットに接続された通信装置であっても暗号装置を介することにより、同一社内で1つのグループを形成し、通信データのやりとりは暗号化することができる。そのため、インターネットを介した通信であっても、盗聴を防ぐことができる。

【0087】図14は、暗号化システムを用いた他のネットワーク例である。LAN/WAN15に、LAN1がルータ14を介し3本接続されている。LAN1には、暗号装置81～85が接続されている。通信端末21～29は、暗号装置に接続されている。通信端末20は、暗号装置を介さず、LAN1に接続されている。人事ファイルサーバ99は、暗号装置83に接続されてい

る。

【0088】図14のネットワーク例において、暗号装置84の暗号化条件を次のように設定する。

基本バス：アプリケーション（全）；セッション鍵Aにより暗号

特例1：IPアドレス（人事ファイルサーバ）&アプリケーション（全），セッション鍵Bにより暗号

【0089】図14において、グループAは、セッション鍵Aによるグループである。例えば、技術部のグループとする。グループBは、セッション鍵Bによるグループである。例えば、これを人事部とする。グループBには、人事ファイルサーバ99があり、一般的のアクセスは禁止したい。上記のように、暗号化条件を設定すると、通信端末27からセッション鍵Aを用いると、グループA内の全ての通信端末と全てのアプリケーションについて通信データを送受信できる。通信端末27からは、セッション鍵Bを用いて人事部、即ち、グループBの人事ファイルサーバ99と全てのアプリケーションに関し、通信データを送受信できる。そのため、通信端末27のユーザを人事権のある役員とする。このように、暗号装置に複数のセッション鍵を保有し、暗号化条件でどのセッション鍵を使用するか設定することにより、いろいろなグループの組み合わせを重複して作ることができる。そのため、セッション鍵による暗号化条件の設定により盗聴防止及びアクセス制御ができ、人事課や役員しかアクセスできない人事情報サーバなどを社内LANに接続できる。

【0090】図15は、暗号化システムを用いた他のネットワーク例である。WAN17は、ルータ14を介し、2本のLAN1と接続されている。それぞれのルータ14のLAN1側に、暗号装置81と82を接続する。これにより、例えば、社内全体を1つのグループ、グループAとすることができる。2本のLAN1には、暗号装置83と84がそれぞれ接続されている。暗号装置83と84には、通信端末23、24、27、28が接続されている。しかし、更に、多くの通信端末を暗号装置にそれぞれ接続してもよい。また、LAN1には、暗号装置を介さずに通信端末21、22、25、26が接続されている。しかし、更に、多くの通信端末を接続してもよい。暗号装置83と84及び暗号装置に接続された通信端末でグループBが形成される。グループBを例えば、人事部とする。グループBは、グループAに属する。しかし、暗号装置83、84を介さないグループAの通信端末21、22、25、26からは、グループBの通信端末23、24、27、28と通信データのやりとりをすることはできない。また、通信端末21、22、25、26は、相互に通信データを送受信できるが、通信データは暗号化されない。暗号化されるのは、例えば、通信装置21が通信装置25に通信データを送受信したい場合、通信装置21側のLAN1に接続され

た暗号装置81で暗号化され、WAN17を介し暗号装置82で復号されるまでである。暗号装置82で復号された通信データは、平文通信で通信端末25に届く。即ち、WAN17のような公衆網を通る時に、暗号化され盗聴を防止することができる。このように、暗号装置を配置することにより盗聴を防止できるため、従来専用線でしか構築できなかったシステムが公衆網を利用することができる。

【0091】図16は、アプリケーションとセッション鍵により暗号化条件を定めることにより、重複した複数のグループ化ができるることを説明する図である。暗号装置81～83が、LAN1に接続されている。暗号装置81では、アプリケーション1～4と6を実行する。暗号装置82では、アプリケーション1、3、5、6を実行する。暗号装置83では、アプリケーション1、2、4～6を指定する。同一番号のアプリケーションが登録されている暗号装置間では、同じセッション鍵で通信データを暗号化／復号する。これにより、アプリケーション1、6が指定されている暗号装置81～83で、グループAが形成される。アプリケーション2、4が指定されている暗号装置81、83で、グループBが形成される。アプリケーション3が指定されている暗号装置81、82で、グループCが形成される。アプリケーション5が指定されている暗号装置82と83で、グループDが形成される。このように、暗号化条件の指定の仕方により、上記のように、3台の暗号装置を様々に組み合わせ、重複した複数のグループを形成することができる。なお、この例では、アプリケーションを例としたが、通信プロトコルのタイプによりグループ化してもよい。暗号装置に1つのセッション鍵しか保有できない場合、暗号装置とセッション鍵が1対1で対応するので、セッション鍵をどの暗号装置に持たせるかにより、暗号装置のグループ化をする。この場合、物理的ネットワークのグループを形成することができる。暗号装置に複数のセッション鍵を保有できる場合は、アプリケーションや通信プロトコルなどの機能とセッション鍵の組み合わせにより、1台の暗号装置が重複して複数のグループに属することができる。これは、物理的ネットワークグループに対し、論理的ネットワークグループということができる。

【0092】図17は、図11で鍵管理装置6aがセッション鍵は生成するが、暗号装置81a、82aにネットワークを介して配達しない場合のブロック図を示す。暗号化条件の設定及び暗号化条件の判定は、上述した通りである。

【0093】図18は、図11において、鍵管理装置を省く場合のブロック図である。各暗号装置で保有するセッション鍵は、鍵管理装置6のセッション鍵生成手段31と同等の機能を有する図示していない処理装置で作成し、暗号装置81bのセッション鍵記憶手段711に入

力し記憶される。この場合も複数のセッション鍵を作成し、セッション鍵記憶手段 711 に記憶することは可能である。暗号装置 81b, 82b は、セッション鍵記憶手段 711, 721、暗号処理手段 413, 423、データ送受信手段 414, 424、暗号化条件記憶手段 811, 821、条件判定手段 812, 822 からなる。暗号化条件は、それぞれ暗号装置のユーザが暗号化条件記憶手段 811, 821 に記憶する。暗号化条件による論理的ネットワークグループの形成は、上記説明と同様である。なお、上記実施の形態で述べたモードスイッチを暗号装置に備えてもよい。この場合、暗号化条件がどのようなものであっても、モードスイッチが ON であれば、平文通信に切り換わるとする。

【0094】以上のように、この暗号化システムを用いることにより、専用線でしか構築できなかった盗聴防止システムが、公衆網やインターネットを利用して構築することができる。また、ネットワークを使った情報サービスにおいて、暗号鍵を持つユーザのみがアクセスすることができるグループ化を図ることができる。また、人事課や役員しかアクセスできない人事情報サーバなどを社内 LAN に接続できる。この場合、暗号化条件の設定により一般のユーザが人事情報サーバを盗聴することができないし、アクセスすることもできない。また、暗号化条件の機能（通信プロトコル、アプリケーション）とセッション鍵の指定の仕方により、複数の重複した論理グループを同一のネットワーク上に構築することができる。

【0095】実施の形態 3. この実施の形態は、1 台の暗号装置に複数の通信端末が接続される場合、通信端末を接続するポート毎に暗号化のための条件を基本バスと特例バスにより設定することができる暗号化システムについて述べる。

【0096】図 19 は、この実施の形態で用いるネットワークシステムを示す図である。図において、暗号装置 81～84 は、通信端末が 1 台接続される NODE 型暗号装置である。暗号装置 51, 52 は、通信端末が複数台接続される HUB 型暗号装置である。暗号装置 81、暗号装置 51、暗号装置 82 は、これらの暗号装置に接続される通信端末 20～23, 25 とともに、グループ A を形成する。暗号装置 83, 84 と暗号装置 52 は、それぞれに接続される通信端末 26～29 とともに、グループ B を構成する。鍵管理装置 7 は LAN 1 に接続され、暗号装置 81～84 と暗号装置 51, 52 の暗号化／復号に用いるセッション鍵を生成し、各暗号装置に配布する。また、通信端末 24 は、平文通信のみ行える端末である。

【0097】図 20 に、1 台の暗号装置に 1 台の通信端末が接続される NODE 型暗号装置 81 を示す。暗号装置 81 には、平文ポートと暗号ポートがあり、平文ポートには、通信端末 20 が 1 台接続される。通信端末 20

と暗号装置 81 の間をながれるデータは、暗号化されない平文である。暗号装置 81 の暗号ポートは、LAN 1 に接続される。暗号ポートを流れるデータは、暗号化されたデータである場合もあるし、平文の場合もある。NODE 型暗号装置は、接続の制限として平文ポート側に 1 台の通信端末のみが接続され、別の HUB やブリッジ／ルータの接続は、禁止である。また、暗号化条件で指定する通信方向は、平文ポートから暗号ポートにデータが流れる方向を（出）、即ち、出方向と定義する。図 21 に、1 台の暗号装置に複数台の通信端末が接続される HUB 型暗号装置 51 を示す。暗号装置 51 の平文ポートには、通信端末 21, 22, 23 が接続される。暗号装置 51 の暗号ポートは、LAN 1 に接続される。HUB 型暗号装置の接続の制限としては、平文ポート側には複数のポートを備え、1 つのポートに 1 台の端末のみが接続され、別の HUB やブリッジ／ルータの接続は、禁止である。暗号化条件で用いる通信方向（出）は、図に示すように、平文ポートから暗号ポートへ流れる方向とする。

【0098】図 22 は、この実施の形態で用いる鍵管理装置 7 と暗号装置 81, 暗号装置 51、通信端末 20～23 のブロック図である。鍵管理装置 7 は、上記実施の形態で述べた図 11 における鍵管理装置 6 に、ポート条件設定手段 63 が加わったものである。暗号装置 51 は、通信端末 21～23 が接続される HUB 型暗号装置である。暗号装置 51 は図 11 における暗号装置 82 の暗号化条件記憶手段 821 が、ポート条件記憶手段 921 に置き換わったものである。ポート条件記憶手段 921 は、通信端末を接続するポート毎に、上記実施の形態で述べた基本バスと特例バスをポート条件として記憶する。条件判定手段 822 は、ポート条件記憶手段 921 に設定されているポート条件と通信端末 21～23 より入力された通信データの条件（通信データを用いるアプリケーション、通信方向、通信相手となる通信装置）とを比較し、ポート条件記憶手段 921 に記憶された基本バスと特例バスの中の何れのバスを用いるか判定し、基本バス、あるいは、特例バス用に設定されたセッション鍵で暗号化するか、あるいは、平文通信とするか決定する。暗号装置 81 は、通信端末 20 を 1 台接続する NODE 型暗号装置である。入出力装置 5 と暗号装置 81 と通信端末 20～23 は、図 11 と同様である。

【0099】鍵管理装置 7 におけるポート条件設定手段 63 は、鍵管理者が HUB 型暗号装置のポート条件を設定し、対象となる HUB 型暗号装置 51, 52 におけるポート条件記憶手段 921 に配布する。しかし、暗号装置 51, 52 において、それぞれポート条件を設定し、ポート条件記憶手段 921 に設定するならば、鍵管理装置 7 におけるポート条件設定手段 63 は省いてよい。しかし、鍵管理装置 7 のポート条件設定手段 63 で、暗号装置のポート条件を設定すること

によりポート条件の一括管理が可能となる。セッション鍵記憶手段 711, 721 は、鍵管理装置 7 のセッション鍵生成手段 31 で生成された鍵と、暗号化条件記憶手段 811 またはポート条件記憶手段 921 に設定される鍵の識別子との対応を記憶する。例えば、暗号化条件記憶手段 811 に記憶される基本バス用と特例バス用のセッション鍵として鍵A, 鍵B, 鍵Cと記述する。セッション鍵記憶手段 711, 721 には、セッション鍵の識別子、鍵 A, 鍵 B, 鍵 C とそれぞれに対応する鍵管理装置 7 から配達されたセッション鍵を記憶する。このようにすることにより、暗号化条件とポート条件を設定する鍵管理者が実際のセッション鍵を知る必要がない。また、セッション鍵の秘密性を守るために、定期的にセッション鍵を鍵管理装置 7 で生成し変更する場合、暗号化条件とポート条件にセッション鍵の識別子で指定するため、暗号化条件とポート条件をセッション鍵の更新の度に変更する必要がない。

【0100】図 23 に、暗号化条件記憶手段 811 に記憶する暗号化条件の例を示す。図 23 の暗号化条件を以下に記す。

基本バス：アプリケーション（全），鍵 A

特例バス 0：宛先 IP アドレス（全）&アプリケーション（メール），透過

特例バス 1：宛先 IP アドレス（通信端末 26）&アプリケーション（AP11）&通信方向（出），鍵 B
このように、暗号化条件としては、基本バスと特例バスを記憶することができる。基本バスは、デフォルトとして扱われるバスで、特例バスに合致しない通信は全て基本バスで扱われる。そのため、宛先 IP アドレスの指定はできない。一方、特例バスは、宛先 IP アドレスを必ず設定し、特例バスで設定された条件に合致する通信は、該当特例バスで設定されたセッション鍵により暗号化される。あるいは、透過設定された場合は、暗号化せず、平文のまま暗号装置から出力される。暗号化条件として、特例バスは必ずしも指定しなくてもよい。即ち、暗号化条件は、少なくとも基本バスを設定しなければならない。なお、基本バスと特例バスに合致しない通信は、全て廃棄される。

【0101】次に、基本バスと特例バスの特徴をそれぞれ述べる。基本バスは、NODE 型暗号装置では、平文ポートが 1 つなので 1 つ設定可能である。基本バスでは、宛先 IP アドレスは指定できないが、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。アプリケーションフィルタは、特定のアプリケーション名の指定が可能であり、その他全通過、あるいは、全廃棄の指定が可能である。また、データを暗号装置の平文ポートから暗号ポートへ出力するか、又は、逆方向に入力するかによる通信方向フィルタの設定ができる。通信方向は、図 20、図 21 に示したように、平文ポートから暗号ポートへデータが流れる方

向を出方向（出）とする。反対に、暗号ポートから平文ポートへデータが流れる場合、入方向（入）とする。更に、出方向及び入方向を合わせた両方向の指定が可能である。両方向を指定する場合は、基本バス及び特例バスに通信方向を明記しなければ、両方向扱いとなる。セッション鍵は、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する場合に用いる。セッション鍵は、基本バスの場合、暗号装置の属するグループの鍵に固定される。また、セッション鍵を指定せず、透過設定（平文通信）とすることも可能である。

【0102】特例バスは、複数種類設定することが可能であり、この実施の形態では、1 台の暗号装置で最大 64 設定することができる。特例バスでは、宛先 IP アドレスフィルタ、アプリケーションフィルタ、通信方向フィルタ、セッション鍵を指定することができる。特例バスでは、宛先 IP アドレスを指定しなければならない。また、IP アドレスの有効ビット長も併せて指定する。暗号化条件の通信相手として IP アドレスと IP アドレスの有効ビット長という 2 項目を設定する。IP アドレスは、4 つの数字をドット（.）で区切って表現する。各数値は、0 ~ 255 までの範囲を取ることが可能である。0 ~ 255 の数値は、2 進数で表現すると 8 ビットで表すことができるので、有効ビット長により（8 ビット × 4）桁の内、どこまでのビットをそのまま使用するのかを指定する。有効ビット長で範囲外とされたビットは 0 であると見なす。例えば、133.141.70.151 という IP アドレスで、有効ビット長 = 32 ビットの場合は、通信相手となる通信装置は 1 つだけで、133.141.70.151 の IP アドレスを持つ通信装置となる。しかし、同じ 133.141.70.151 という IP アドレスで、有効ビット長 = 24 ビットとすると、133.141.70.0 ~ 133.141.70.255 までの 256 通りの IP アドレスのうちいずれかの IP アドレスを持つ複数の通信装置が通信相手となる。このように、IP アドレスの有効ビット長指定により通信相手となる通信装置は 1 つであったり、複数であったりする。特例バスのアプリケーションフィルタ、通信方向フィルタを設定するための仕様は基本バスと同じ仕様である。セッション鍵は、宛先 IP アドレスフィルタ、アプリケーションフィルタ、通信方向フィルタの各条件に合致した通信を暗号化する。セッション鍵は、セッション鍵記憶手段 711 に複数のセッション鍵を記憶することにより、複数のセッション鍵の中から 1 つを選んで特例バスに指定することができる。セッション鍵は、特例バス毎に 1 個指定する。または、セッション鍵を設定せず平文通信とする透過設定にすることも可能である。また、特例バスでは、宛先 IP アドレスを指定するという特性から、例えば、IP ブロードキャストアドレスは、扱うことができない。即ち、ブロードキャ

ストを使用するようなアプリケーションは、特例バスでは扱えず、基本バスの中で扱うことになる。

【0103】図24に、ポート条件記憶手段921に記憶するポート条件の例を示す。図24におけるポート条件を以下に記す。

ポート1

基本バス1：アプリケーション（全），鍵A

ポート2

基本バス2：アプリケーション（メール），透過

特例バス1：宛先IPアドレス（通信端末26）&アプリケーション（AP11）&通信方向（出），鍵B

ポート3

基本バス3：アプリケーション（AP22）&通信方向（入），鍵A

特例バス1：宛先IPアドレス（通信端末26）&アプリケーション（AP11）&通信方向（出），鍵B

特例バス2：宛先IPアドレス（通信端末28）&アプリケーション（SPPR），鍵C

【0104】HUB型である暗号装置51は、複数のポートを備え、図22の例では、3台の通信端末21～23が接続されている。そのため、ポート1、ポート2、ポート3毎に、それぞれポート条件を記憶する。ポート条件としては、基本バスと特例バスを指定することができる。基本バスと特例バスの特徴は、上述した通りであるが、NODE型暗号装置とHUB型暗号装置では次のような相違がある。NODE型暗号装置における基本バスは、装置当たり1つ指定する。HUB型暗号装置では、ポート毎に1つの基本バスを設定する。特例バスは、HUB型暗号装置では、複数ポートで共有可能である。ポート条件として、特例バスは必ずしも指定しなくてもよい。即ち、ポート条件は、各ポート毎に少なくとも基本バスを設定しなければならない。

【0105】特例バスと基本バスの優先順位は、特例バスが優先される。また、特例バスが複数ある場合は、特例バスそれぞれに予め優先順位を与えておくことができる。この実施の形態では、暗号条件記憶手段、ポート条件記憶手段に記憶する特例バスの順番で優先順位を与える。

【0106】図25に、図24に示したポート条件を例にポート条件における基本バスと特例バスの関係を述べる。図25に示す模式図では、ポート1は、基本バスだけである。ポート2は、基本バスと特例バス1、ポート3は、基本バスと2つの特例バス1、2を持つ。また、特例バス1は、ポート2とポート3で共有しているところを示している。更に、パイプの途中に挿入されている横円形のふるいに当たる部分が、各種の選択処理を表している。図の横円形に（ ）内に記したものは、図24のポート条件である。例えば、特例バス2を例にとると、宛先IPアドレスフィルタにおける（28）は、通信端末28を示す。アプリケーションフィルタ（SPP

R）は、アプリケーションSPPRを表す。通信方向フィルタにおける（両）は、通信方向が両方向であることを示す。セッション鍵（C）は、セッション鍵の識別子として鍵Cを示す。また、基本バス1、3で指定するセッション鍵は、暗号装置が属するグループのセッション鍵Aであり、固定である。基本バス2には透過を設定する。

【0107】基本バスと特例バスをこのように設定することができるため、暗号化することによるセキュリティ強化とともに、ユーザの利便性を考慮していくつかの選択性を提供することができる。例えば、通常暗号ワールドにいるユーザがネットニュースを平文で運用したいという要望に答え、ニュースサーバとの通信だけ例外的に平文で行うことが可能となる。また、特例バスを用い、グループに与えられたセッション鍵以外のセッション鍵を指定することができるため、予め設定されたグループを物理グループとすると、この物理グループに属しながら新たな論理グループを形成することができる。新たな論理グループを形成する条件は、宛先IPアドレス、アプリケーション、通信方向、セッション鍵であり、これらの組み合わせにより設定することができる。

【0108】図26に、図19に示したネットワークシステムにおいて、暗号装置81、51で図23、図24に示す暗号化条件とポート条件を設定することにより形成される新たな論理グループを示す。グループAに属する通信端末20、22、23は、特定のアプリケーション（AP11）の場合、通信端末26に通信データを出力することができる。通信端末20、22、23は、グループAに属するが、特例バス1を設定することによりグループBの通信端末26と新たな論理グループ1を形成する。論理グループ1は、アプリケーション（AP11）を通信端末20、22、23で処理しているときに形成されるグループである。また、更に、論理グループ1は、通信方向が通信端末20、22、23から通信端末26に出力される場合に限り形成されるグループである。論理グループ2は、図24のポート3における特例バス2で設定された条件により生ずるグループである。この場合、論理グループ2は、通信端末23において、アプリケーション（SPPR）が実行される際、通信端末28とデータのやりとりをする場合に生じるグループである。このように、特例バスの設定により予め定められたグループを越えて新たな論理グループを形成することが可能となる。また、特例バスの設定の仕方により、例えば、グループAの中に1以上のサブグループを形成することも可能となる。また、1台の暗号装置に複数台の通信端末が接続されていても、ポート毎にポート条件を設定することにより各通信端末毎に異なった使い方が可能となる。例えば、図24の例であると、通信端末21は、グループAにのみ属する。通信端末22は、基本的には、アプリケーション（メール）のための通信端末

とし、他のアプリケーション（メール）を行う通信端末と、グループ分けに関わらずデータ交換が平文で可能となる。また、通信端末22は、アプリケーション（A P 1 1）を実行する際、通信端末22から通信端末26にデータを送信する端末となる通信端末23は、アプリケーション（A P 2 2）を行う場合、他の通信端末から通信を受信する端末として基本的に動作する。また、アプリケーション（A P 1 1）を実行し、通信端末26にデータを送信する端末となる。また、アプリケーション（S P P R）を実行することができ、通信端末28と通信のやりとりを行うことができる端末である。このように、1つの暗号装置に接続されていながら、各通信端末毎にそれぞれ性格の異なる役割を分担することが可能となる。

【0109】図27は、HUB型暗号装置を用いた通信形態の例を示す。暗号装置51のもとに、通信端末21、22が接続され、暗号装置52のもとに、通信端末23とDBサーバ904が接続され、セッション鍵1によるグループ1が形成される。暗号装置53のもとに、通信端末24、25が接続され、暗号装置54のもとに、通信端末26とDBサーバ905が接続され、セッション鍵2によりグループ2を形成する。暗号装置51～54は、HUB型暗号装置である。暗号装置51のポート2に接続された通信端末22がEOAサーバ901、ニュースサーバ902、WWWサーバ903とは、平文通信を行い、かつ、DBサーバ905とは暗号通信を行う。この場合暗号装置51に、図28に示すポート条件（ポート2のみを記す）を設定する。

基本バス：アプリケーション（全），鍵1

特例1：宛先IPアドレス（aaa）&アプリケーション（A P 2 3）&通信方向（出），透過

特例2：宛先IPアドレス（bbb）&アプリケーション（A 1 1 9）&通信方向（出），透過

特例3：宛先IPアドレス（ccc）&アプリケーション（T 8 0）&通信方向（出），透過

特例4：宛先IPアドレス（ddd）&アプリケーション（A P 1 5 2 3）&通信方向（出），鍵2

【0110】ここで、aaaはEOAサーバのIPアドレスであり、bbbはニュースサーバのIPアドレスであり、cccはWWWサーバのIPアドレスであり、dddはDBサーバ905のIPアドレスである。基本バスは、グループ1に属することを定義し、全てのアプリケーションについて、かつ、両方向通信について、セッション鍵1で暗号化／復号を行うことを意味する。特例バス1は、EOAサーバと平文通信を行うための設定である。特例バス2は、ニュースサーバと平文通信を行うための設定である。特例バス3は、WWWサーバと平文通信を行うための設定である。特例バス4は、DBサーバ905とセッション鍵2により暗号通信を行うための設定である。

【0111】図29に、LANに接続する暗号装置を示す。LANに接続する暗号装置501は、平文ポートから入力された暗号化されていないデータを暗号化し、暗号ポートから出力する。図30と図31に、LANに接続する暗号装置501の設置例を示す。図30では、ルータ142と広域網に接続されたルータ141側に暗号装置501の暗号ポートを接続する。暗号装置501の平文ポートには、ルータ143とブリッジ151が接続される。ルータ143とブリッジ151から入力される暗号化されていないデータが、暗号装置501の平文ポートに入力され、暗号装置501で暗号化されて暗号ポートから出力される。暗号化されたデータは、ルータ141を介し広域網を通り、通信相手先へ通信される。または、暗号化されたデータは、ルータ142を介し通信相手先へ通信される。図31は、LANに接続する暗号装置501、502の第2の設置例である。広域網にルータ141が接続され、ルータ141にイーサネット・スイッチ131、132が接続される。イーサネット・スイッチ131の1つのポートに、LANに接続する暗号装置501の暗号ポートが接続される。暗号装置501の平文ポートが、一般HUB121に接続される。暗号装置502に関する同様である。一般HUB121、あるいは、122から入力される暗号化されていないデータが暗号装置501、あるいは、502の平文ポートに入力され、暗号化されて暗号ポートからイーサネット・スイッチ131、あるいは、132に出力される。暗号装置501、502の暗号ポート側、即ち、イーサネット・スイッチ131、132とルータ141を介した広域網側では、暗号化されたデータとなる。

【0112】図32は、LANに接続する暗号装置を用いた通信形態を示す図である。子会社Aと子会社Bと本社は、インターネット16を介し通信を行う。子会社Aは、暗号装置501をインターネット16側のルータ143に接続する。子会社Bは、暗号装置502をインターネット16側のルータ144に接続する。本社は、暗号装置503をインターネット16側のルータ145に接続する。これにより、本社、子会社A、子会社Bとの間で通信を行う場合、暗号装置501、502、503によりインターネット側では通信データが暗号化されるため、通信のセキュリティが保たれる。本社と子会社Aとは、セッション鍵5を用いた通信を行う。本社は、子会社Bとはセッション鍵6を用いてWWWサーバアクセスだけを行う。また、本社からインターネット16上の各種公開サーバ906とは、平文でアクセスを行いたい。このような通信形態を行う際の本社にある暗号装置503での暗号化条件を、図33に示す。

基本バス1：アプリケーション（全），透過

特例1：IPアドレス（aaa）&アプリケーション（全），鍵5

特例2：IPアドレス（bbb）&アプリケーション

(A P 8 0) & 通信方向 (出), 鍵 6

ここで、aaaは子会社Aに設置されたルータ141のIPアドレスである。bbbは子会社Bに設置されたルータ142のIPアドレスである。なお、LANに接続する暗号装置には、平文ポートが1本なのでポート条件ではなく、暗号化条件を記憶する。

【 0 1 1 3 】 以上のように、この実施の形態では、1台の暗号装置が複数のポートを備え、それぞれのポートに通信端末が複数接続される場合、ポート毎に暗号化に関するポート条件を記憶することができる暗号化システムについて述べた。これにより、暗号通信、平文通信を設定できるとともに、宛先IPアドレス、アプリケーション、通信方向、セッション鍵によりポート毎に暗号化する条件を設定することができる。そのため、予め設定された通信装置からなる物理グループの暗号化通信以外に、柔軟に宛先IPアドレス、アプリケーション、通信方向、セッション鍵により新たな論理グループを設定することができる。また、同じ暗号装置に接続される通信端末であっても、それぞれのポート条件を変えることができるため、通信端末を1台毎に異なった使い方ができ、ユーザにとって使いやすい暗号化システムを提供することができる。

【 0 1 1 4 】 実施の形態4. この実施の形態は、鍵管理装置と暗号装置と通信端末により暗号管理ドメインを形成し、複数の暗号管理ドメイン間で共通セッション鍵を持つことにより、異なる暗号管理ドメイン間の暗号化通信が可能な暗号化システムについて述べる。また、暗号化条件とポート条件に共通セッション鍵を設定することにより、異なる暗号管理ドメインに属する通信端末からなる論理グループを形成する暗号化システムについて述べる。

【 0 1 1 5 】 図34は、この実施の形態における暗号化システムのネットワークシステムを示す図である。暗号管理ドメインA, B, Cに分けられ、それぞれ1台の鍵管理装置と複数台の暗号装置と複数台の通信端末とからなる。暗号管理ドメイン間は、ルータ14とLAN/WAN15によりネットワーク接続されている。暗号管理ドメインA～Cは、通常それぞれに属する鍵管理装置71～73がセッション鍵を生成し、管理するため、暗号管理ドメイン相互間の暗号化通信はできない。そこで、共通セッション鍵を複数の暗号管理ドメインで共有することにより、暗号管理ドメイン間の暗号化通信を行う。この実施の形態では、複数ある鍵管理装置の内、1台の鍵管理装置をマスタ鍵管理装置とし、共通セッション鍵を生成し、他の鍵管理装置に配送する。ここでは暗号管理ドメインAの鍵管理装置71をマスタ鍵管理装置とし、共通セッション鍵を生成し配送するものとする。鍵管理装置72及び鍵管理装置73を鍵管理装置71から共通セッション鍵を受け取る鍵管理装置とする。なお、共通セッション鍵に対し、暗号管理ドメイン内で用いる

セッション鍵をローカル鍵と呼ぶこととする。

【 0 1 1 6 】 図35に、鍵管理装置71, 72のブロック図を示す。鍵管理装置71, 72には、図22に示した鍵管理装置7にセッション鍵テーブル64が加わる。鍵管理装置71, 72におけるセッション鍵生成手段31が複数のセッション鍵を生成し、セッション鍵テーブル64に記憶する。この実施の形態では、鍵管理装置71～73でそれぞれ最大32個のセッション鍵を生成するものとする。図36に、セッション鍵テーブル64の例を示す。セッション鍵テーブル64は、鍵番号と、鍵作成可否を示す許可フラグと、生成された鍵と、その鍵に対する属性を記憶する欄がある。鍵番号1から鍵番号32に対応して、共通セッション鍵とローカル鍵を鍵の欄に記憶する。セキュリティ強化のため一定時間毎にローカル鍵は生成され、更新される。共通セッション鍵は更新不可のため、許可フラグを「非作成」(図では×で示す)とする。共通セッション鍵に対し暗号管理ドメインA, B間の共通セッション鍵であることを記憶するために属性欄に"共通(A, B)"と書き込まれている。鍵管理装置72は、図22の鍵管理装置7にセッション鍵テーブル64に加え、更に、セッション鍵受信手段65とセッション鍵復号手段66が加わったものである。セッション鍵受信手段65とセッション鍵復号手段66は、鍵管理装置71から暗号化されて配送される共通セッション鍵を受信し、復号する。なお、鍵管理装置71～73の通信装置グループ記憶手段37は、暗号管理ドメインA～C毎に鍵管理装置と暗号装置と通信端末のアドレスを記憶する。他の構成要素は、上記実施の形態で述べた構成要素と同様であるので、説明は省略する。また、NODE型暗号装置81～88とHUB型暗号装置51～54は、図22で述べたブロック図と同様であるので、説明は省略する。

【 0 1 1 7 】 暗号管理ドメインAでは、鍵管理装置71が共通セッション鍵とローカル鍵を複数生成し、暗号管理ドメインAに属する暗号装置81～83と暗号装置51に配送する。また、共通セッション鍵は鍵管理装置72, 73に配送される。更にセキュリティ強化のため、鍵管理装置71はローカル鍵を定期的に生成し、各暗号装置のローカル鍵を更新する。また、鍵管理装置71は、暗号化条件設定手段62により暗号装置81～83の暗号化条件記憶手段811～831に暗号化条件を設定する。鍵管理装置71のポート条件設定手段63は、暗号装置51のポート条件記憶手段921にポート条件を設定する。また、暗号管理ドメインB, Cにおいても、鍵管理装置72, 73が同様に暗号管理ドメイン内で用いるローカル鍵を定期的に生成する。また、共通セッション鍵は鍵管理装置71から配送されたものを使う。鍵管理装置72, 73はローカル鍵と共通セッション鍵を用いて暗号化条件及びポート条件を所属する暗号装置に設定する。

【0118】次に、鍵管理装置71が共通セッション鍵を生成し配達する手順を述べる。初めに、暗号管理ドメインAと暗号管理ドメインBとの間で鍵番号5, 8, 3-2を共通セッション鍵1～3とすると、取り決めである場合について述べる。

(1) 鍵管理装置71のセッション鍵生成手段31が32個のセッション鍵を生成する。

(2) セッション鍵生成手段31でセッション鍵が32個生成されると、セッション鍵管理手段32は、セッション鍵テーブル64に作成したセッション鍵を書き込む。セッション鍵管理手段32は、セッション鍵テーブル64の鍵番号5, 8, 32に対応する許可フラグを「非作成」とする(図では、×印)。更に、鍵番号5, 8, 32に対応する属性欄に、暗号管理ドメインAと暗号管理ドメインB間の共通セッション鍵であることを示す“共通(A, B)”を書き込む。

(3) セッション鍵管理手段32は、暗号管理ドメインBに生成した共通セッション鍵1～3を配達するため、セッション鍵暗号化手段34で共通セッション鍵1～3を暗号化し、セッション鍵送信手段35で、暗号管理ドメインBの鍵管理装置72へ送信する。

【0119】(4) 暗号管理ドメインBの鍵管理装置72におけるセッション鍵受信手段65は、鍵管理装置71のセッション鍵送信手段35から送信された、暗号化された共通セッション鍵1～3を受信する。鍵管理装置72におけるセッション鍵管理手段32は受信された、暗号化された共通セッション鍵をセッション鍵復号手段66に渡す。セッション鍵復号手段66は、暗号化された共通セッション鍵を復号する。鍵管理装置72におけるセッション鍵管理手段32は、復号された共通セッション鍵をセッション鍵テーブル64の鍵番号5, 8, 32に対応する鍵の欄に書き込み、許可フラグを「非作成」とする。また、セッション鍵テーブル64の鍵番号5, 8, 32に対応する属性欄に、暗号管理ドメインAと暗号管理ドメインB間の共通セッション鍵であることを示す“共通(A, B)”を書き込む。鍵管理装置72のセッション鍵テーブル64において、鍵番号5, 8, 32に既に共通セッション鍵が書かれている場合は、上書きされる。

(5) 鍵管理装置72のセッション鍵生成手段31は、自暗号管理ドメインのためのローカル鍵を生成する。セッション鍵管理手段32は、セッション鍵テーブル64の許可フラグが「作成」(図では、○印)となっている鍵番号に、セッション鍵生成手段31が生成したセッション鍵をローカル鍵として書き込む。鍵管理装置71, 72のローカル鍵は、上記実施の形態で述べたと同様な方法で自暗号管理ドメインの暗号装置に配達される。

【0120】次に、鍵管理装置71が共通セッション鍵を生成し配達する他の手順について述べる。暗号管理ドメインA, B, Cで暗号通信するための共通セッション

鍵を共通セッション鍵1とする。暗号管理ドメインA, Bが暗号通信するための共通セッション鍵を共通セッション鍵2とする。暗号管理ドメインA, Cが暗号通信するための共通セッション鍵を共通セッション鍵3とする。暗号管理ドメインB, Cが暗号通信するための共通セッション鍵を共通セッション鍵4とする。この場合、鍵管理装置71が共通セッション鍵1～4を生成し、暗号管理ドメインBの鍵管理装置72に共通セッション鍵1, 2, 4を配達する。暗号管理ドメインCの鍵管理装置73には、共通セッション鍵1, 3, 4を配達する。初めに述べた方法では、鍵管理装置71と72の間で鍵番号5, 8, 32を共通セッション鍵を登録する鍵番号と決めていた。しかし、ここでは、例えば、鍵管理装置71が生成した32個のセッション鍵の中から任意に4個の共通セッション鍵1～4を選び出し、該当する許可フラグを「非作成」とする。鍵管理装置71は、セッション鍵テーブル64の属性欄にどの暗号管理ドメイン間の共通セッション鍵とするかを書き込む。更に鍵管理装置71は、該当する鍵管理装置に鍵番号と共通セッション鍵と属性情報を配達する。配達された鍵管理装置では、セッション鍵テーブル64の鍵番号の位置に共通セッション鍵を書き込み、許可フラグを「非作成」とし、属性にどの暗号管理ドメインとの共通セッション鍵かを書き込む。このような方法で、各暗号管理ドメインに共通セッション鍵を配達管理してもよい。

【0121】暗号管理ドメインB, Cで、それぞれ必要とする共通セッション鍵1～4を配達された後、各鍵管理装置71～73は、上記実施の形態3で述べたように、自暗号管理ドメイン内の暗号装置に対し、暗号化条件設定手段62とポート条件設定手段63を用いて暗号化条件とポート条件を設定する。暗号化条件とポート条件における基本バスと特例バスの設定については、上記実施の形態と同様であるので説明は省略する。図37に、共通セッション鍵1～4を用いて暗号化条件とポート条件を設定した場合形成される暗号管理ドメインを越えた論理グループの例を示す。通信端末2c, 2d, 2h, 2kが、共通セッション鍵1により暗号化/復号される暗号通信を行う論理グループ1を形成する。通信端末2a, 2b, 2fが、共通セッション鍵2により暗号化/復号される暗号通信を行う論理グループ2を形成する。通信端末2d, 2l, 2mが、共通セッション鍵3により暗号化/復号される暗号通信を行う論理グループ3を形成する。通信端末2e, 2f, 2j, 2kは、共通セッション鍵4により暗号化/復号される暗号通信を行う論理グループ4を形成する。このように、それぞれ独自のセッション鍵を有する暗号管理ドメイン間で共通セッション鍵を共有することにより、暗号管理ドメインの壁を越えた新たな論理グループが通信端末間で形成される。

【0122】以上のように、この実施の形態では、鍵管

理装置と暗号装置と通信端末とからなる暗号管理ドメインが複数あり、各暗号管理ドメインは、鍵管理装置が暗号管理ドメイン内のローカル鍵を生成し管理する。これらの暗号管理ドメイン間で暗号通信を行うための共通セッション鍵を共有し、かつ、暗号条件とポート条件を共通セッション鍵を用いて設定することにより、異なる暗号管理ドメインに属する通信端末同士が共通セッション鍵で暗号化された暗号通信を行うことができる。また、基本バス及び特例バスの設定において、宛先IPアドレス、アプリケーション、通信方向、セッション鍵を設定することが可能であるため、異なる暗号管理ドメイン間の通信端末間で論理グループを形成することができる。また、宛先IPアドレス、アプリケーション、通信方向で共通セッション鍵による暗号通信を設定することができるため、ユーザサイドの利便性とともに、セキュリティの向上を図ることができる。

【0123】

【発明の効果】以上のように、この発明によれば、グループ化された複数の通信装置間で通信データを暗号化、あるいは、復号することができる。

【0124】また、この発明によれば、モードスイッチの設定により、暗号通信と平文通信とのいずれかを選択することができる。

【0125】また、この発明によれば、暗号装置毎に通信データの暗号化条件を設定することができ、暗号化条件により通信データを暗号化するか否か判定することができる。

【0126】また、この発明によれば、通信相手となる通信装置により暗号化するか否かを設定することができる。

【0127】また、この発明によれば、アプリケーション毎に暗号化するか否かを設定することができる。

【0128】また、この発明によれば、通信方向により暗号化するか否かを設定することができる。

【0129】また、この発明によれば、複数あるセッション鍵の中から暗号化条件に定められたセッション鍵で暗号化、あるいは、復号することができる。また、グループ化された通信装置による暗号グループと平行して暗号グループと異なるセッション鍵によるグループを形成することができる。

【0130】また、この発明によれば、鍵管理装置においてグループ毎に個別のセッション鍵を生成することができる。

【0131】また、この発明によれば、暗号装置で設定されたモードスイッチを有効とするか無効とするかを鍵管理装置から管理することができる。

【0132】また、この発明によれば、鍵管理装置から各暗号装置の暗号化条件を設定することができるため、鍵管理装置において暗号化条件の一括管理ができる。

【0133】また、この発明によれば、鍵管理装置で生

成したセッション鍵を暗号化し、グループに対応付けられた暗号装置に配送することができるため、セッション鍵の設置が自動的にできる。

【0134】また、この発明によれば、複数の暗号管理ドメイン同士で暗号通信を行うことができる。

【0135】また、この発明によれば、暗号化条件により暗号化するか否かを設定することができる。

【0136】また、この発明によれば、暗号化条件を特例バスと基本バスを用いて設定することができる。

【0137】また、この発明によれば、暗号化条件をアプリケーションにより定めることができる。

【0138】また、この発明によれば、暗号化条件を通信方向により定めることができる。

【0139】また、この発明によれば、複数あるセッション鍵の中から任意のセッション鍵を用いて暗号化するか否か定めることができる。

【0140】また、この発明によれば、暗号化条件は、通信相手となる通信装置により設定することができる。

【0141】また、この発明によれば、暗号装置に備えられた1以上のポート毎に基本バスと特例バスを設定することができる。そのため、きめ細かな条件設定ができるので、使い勝手のよい暗号化システムを提供することができる。

【0142】また、この発明によれば、鍵管理装置がポート条件を生成し暗号装置に配布するため、鍵管理装置でポート条件の一括管理ができる。

【図面の簡単な説明】

【図1】この発明の一実施の形態におけるネットワークシステムを示す図である。

【図2】この発明の一実施の形態における暗号化システムのブロック図である。

【図3】図2における暗号化システムのセッション鍵の配送手順を示すシーケンス図である。

【図4】図2における暗号化システムのグループ分けを説明する図である。

【図5】暗号化システムにおける有効無効情報設定用画面の例を示す図である。

【図6】KEYDISTコマンドに設定される内容を示す図である。

【図7】図2の暗号化システムにおけるモードスイッチの情報と有効無効判定手段の論理積の結果を説明する図である。

【図8】図4におけるモードスイッチの切り換えと有効無効情報設定後の平文通信での通信データの流れを示す図である。

【図9】図2における暗号化システムの他の構成を示すブロック図である。

【図10】図2における暗号化システムの他の構成を示すブロック図である。

【図11】この発明の一実施の形態における暗号化シ

システムのブロック図である。

【図 12】 図 11 における暗号化システムのネットワーク例を示す図である。

【図 13】 図 11 における暗号化システムのネットワーク例を示す図である。

【図 14】 図 11 における暗号化システムのネットワーク例を示す図である。

【図 15】 図 11 における暗号化システムのネットワーク例を示す図である。

【図 16】 図 11 における暗号化システムの論理グループを説明するための図である。

【図 17】 図 11 における暗号化システムの他の構成例を示すブロック図である。

【図 18】 図 11 における暗号化システムの他の構成例を示すブロック図である。

【図 19】 この発明の一実施の形態におけるネットワークシステムを示す図である。

【図 20】 NODE 型暗号装置を示す図である。

【図 21】 HUB 型暗号装置を示す図である。

【図 22】 この発明の一実施の形態における暗号化システムのブロック図である。

【図 23】 図 22 における暗号化条件記憶手段に記憶する暗号化条件の例を示す図である。

【図 24】 図 22 におけるポート条件記憶手段に記憶するポート条件の例を示す図である。

【図 25】 図 24 に示したポート条件における基本バスと特例バスの関係を説明する図である。

【図 26】 図 19 に示したネットワークシステムにおいて形成される新たなグループを示す図である。

【図 27】 HUB 型暗号装置を用いた通信形態の例を示す図である。

【図 28】 図 27 における通信端末 22 のポート条件の設定を説明する図である。

【図 29】 LAN に接続する暗号装置の図である。

【図 30】 LAN に接続する暗号装置の第 1 の設置例を示す図である。

【図 31】 LAN に接続する暗号装置の第 2 の設置例を示す図である。

【図 32】 LAN に接続する暗号装置を用いた通信形態を示す図である。

【図 33】 図 32 に示した暗号装置 503 における暗号条件を説明する図である。

【図 34】 この発明の一実施の形態におけるネットワークシステムを示す図である。

【図 35】 この発明の一実施の形態における鍵管理装置のブロック図である。

【図 36】 図 35 に示すセッション鍵テーブルを示す

図である。

【図 37】 図 34 に示すネットワークシステムにおいて暗号管理ドメインを超えたグループの例を示す図である。

【図 38】 従来の暗号通信システムを示す構成図である。

【図 39】 図 38 におけるセッション鍵問い合わせ手段の詳細な構成を示す構成図である。

【図 40】 従来の暗号通信システムにおけるセッション鍵の配送の手順を示すシーケンス図である。

【符号の説明】

1 LAN, 3, 3a, 6, 6a, 7, 71, 72, 73 鍵管理装置、5 入出力装置、12 ルータ/ブリッジ、13 ネットワーク管理装置、14, 141~146 ルータ、15 LAN/WAN、16 インターネット、17 WAN、20~29, 2a~2m 通信端末、31 セッション鍵生成手段、32 セッション鍵管理手段、33 セッション鍵送信開始検出手段、34 セッション鍵暗号化手段、35 セッション鍵送信手段、37 通信装置グループ記憶手段、41, 41a, 41b, 42a, 42b, 43~46, 49, 51~54, 81, 81a, 81b, 82, 82a, 82b, 83~88, 501~503 暗号装置、61 有効無効設定手段、62 暗号化条件設定手段、63 ポート条件設定手段、64 セッション鍵テーブル、65 セッション鍵受信手段、66 セッション鍵復号手段、91 サーバ、92 WWW 代理サーバ、93 WWW、94 メールサーバ、95, 903 WWW サーバ、96 メールサーバ A、97, 98 社内メールサーバ、99 人事ファイルサーバ、121, 122 一般 HUB、131, 132 イーサネット・スイッチ、151 ブリッジ、211, 221 アプリケーション、212, 222 通信制御手段、411, 421 セッション鍵復号手段、412, 422 セッション鍵受信手段、413, 423 暗号処理手段、414, 424 データ送受信手段、711, 721 セッション鍵記憶手段、712, 722 モードスイッチ、713, 723 有効無効判定手段、811, 821 暗号化条件記憶手段、812, 822 条件判定手段、901 EOA サーバ、902 ニュースサーバ、904, 905 DB サーバ。

【手続補正 2】

【補正対象書類名】 図面

【補正対象項目名】 図 10

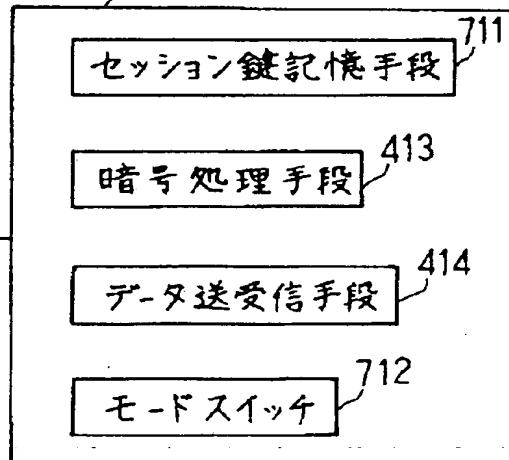
【補正方法】 変更

【補正内容】

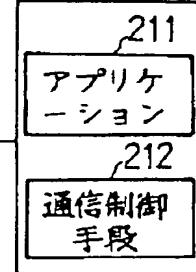
【図 10】

1: LAN

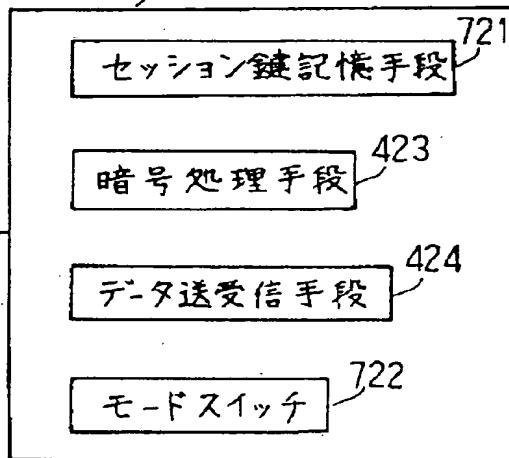
41b: 暗号装置



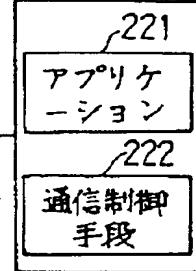
21: 通信端末



42b: 暗号装置



22: 通信端末



【手続補正 3】

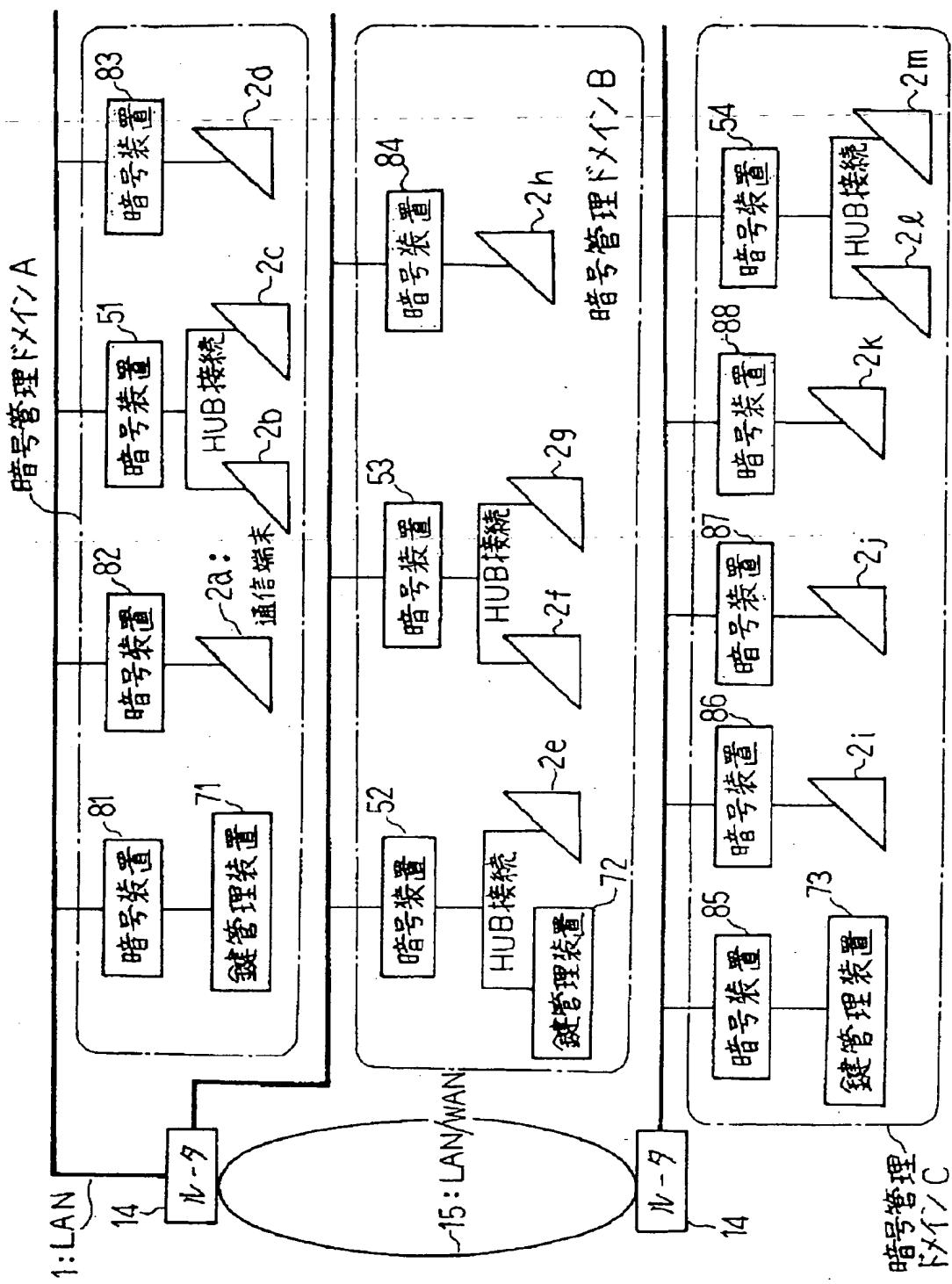
【補正対象書類名】図面

【補正対象項目名】図 34

【補正方法】変更

【補正内容】

【図 34】



【手続補正 4】

【補正対象書類名】 図面

【補正対象項目名】 図 3 6

【補正方法】 変更

【補正内容】

【図 3 6】

鍵番号	許可 フラグ	鍵	属性
1	0	ロ-カル 鍵 1	
2	0	ロ-カル 鍵 2	
3	0	ロ-カル 鍵 3	
4	0	ロ-カル 鍵 4	
5	X	共通セッション鍵1	共通(A,B)
⋮	⋮		
8	X	共通セッション鍵2	共通(A,B)
⋮	⋮		
30	0	ロ-カル 鍵 28	
31	0	ロ-カル 鍵 29	
32	X	共通セッション鍵3	共通(A,B)

【手続補正 5】

【補正対象書類名】図面

【補正対象項目名】図 37

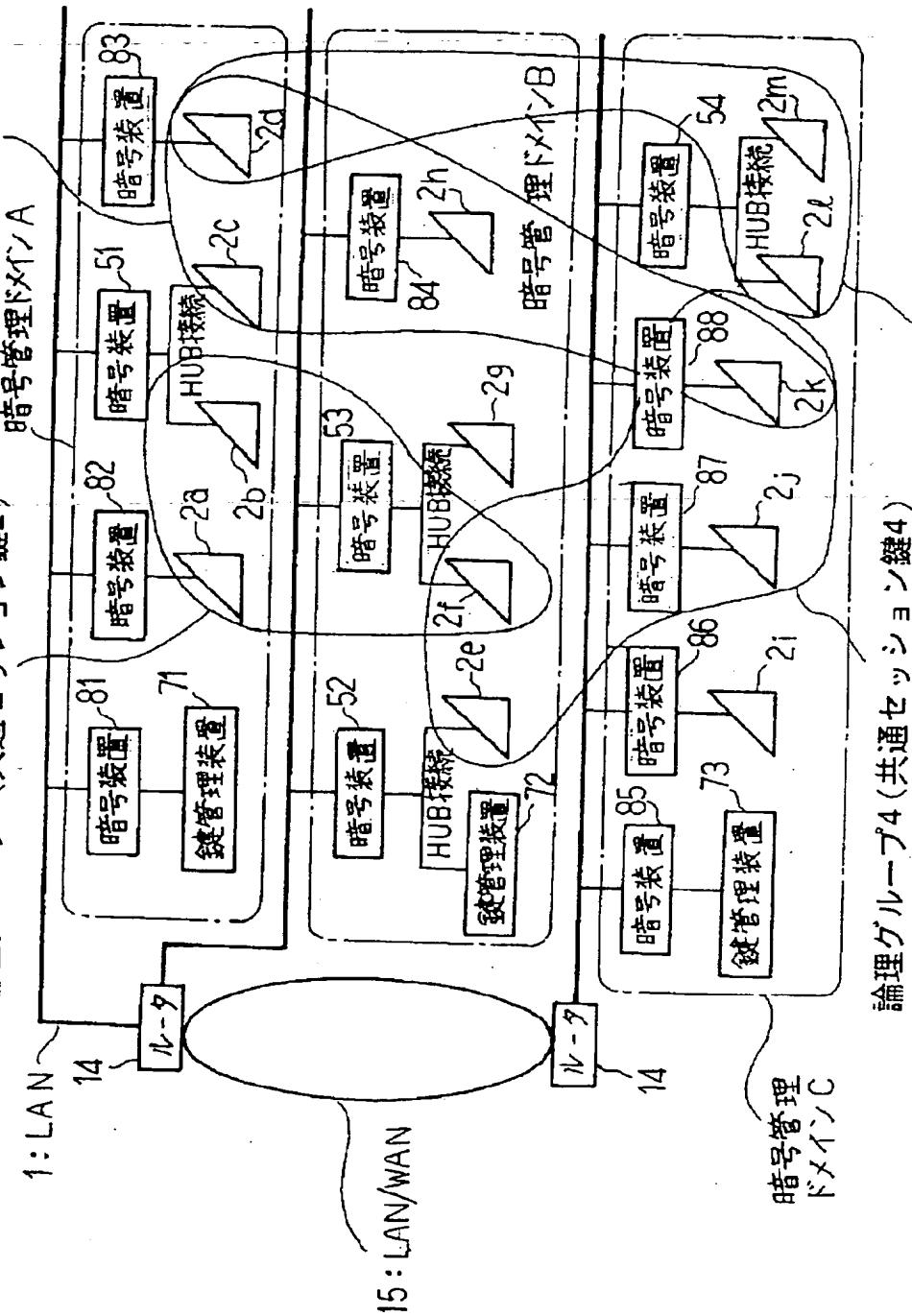
【補正方法】変更

【補正内容】

【図 37】

論理グループ2(共通セッション鍵2)

論理グループ1(共通セッション鍵1)



論理グループ4(共通セッション鍵4)

論理グループ3(共通セッション鍵3)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.